Kirkbie Kendal School Academy Trust

Policy Title:	Data Protection Policy
Policy Reference:	D1
Version:	1.4
Member of Staff Responsible for review:	Data Protection Officer & Headteacher
Governors' Committee/SLT Responsible:	PPM
Status:	Adopted
Date first adopted/accepted by Governing Body:	19 Jun 18
Review Cycle:	2 years
Date of last review:	Mar 22
Date for next scheduled review:	Mar 24

Change Record

Version	Date	Description
1.1	PPM 8 Nov 18	Update to Privacy Notices - requesting access to personal data section in line with DfE update
1.2	FGB 19 Dec 19	Inclusion of Student Friendly version Privacy Notice. Update to Privacy Notices to take account of DfE guidance
1.3	SLT 22 Feb 21 PPM 23 Feb 21	Includes Updated Privacy Notices – Students, student friendly version and Staff – Governors' version – to reflect CV-19 regulations
1.4	SLT 14 March 2022 FGB 16 Mar 22	Title reverted to Data Protection Policy. Updated whole policy with KAHSC v19 Sept 21

"Kirkbie Kendal School promotes the safeguarding and welfare of children in its care; all policies and procedures support the Child Protection Policy."

Contents

1. Introduction

The Data Protection Act 2018 provides a legal framework for data protection in the United Kingdom (UK). It incorporates the General Data Protection Regulations (GDPR), the legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU) and is sometimes referred to as UK GDPR.

UK GDPR significantly updates previous Data Protection law to reflect changes in technology and the way organisations collect and use information about people in the 21st century. It regulates the processing of personal data and gives rights of privacy protection to all living persons.

In accordance with the DPA, we at Kirkbie Kendal School recognise that we collect and process personal data and because we decide how and why we do that, we are *data controllers*. This means that we have legal obligations to people regarding how we handle their data and manage their privacy and we must register as a data controller with the Information Commissioner's Office (ICO Anyone can read the details of our ICO notification by going online to https://ico.org.uk/esdwebpages/search and entering our registration number. Data controllers are normally organisations and not people although our Head teacher is responsible for everything we do day-to-day and we have appointed a Data Protection Officer (DPO).

Our ICO Registration Number is: Z3051354.

Our Data Protection Officer is: Amanda Eastwood.

Contact our DPO on 01539 727422 or email them at: aeastwood@kksa.co.uk

We recognise that when we process personal data it can involve collecting, recording, organising, storing, altering, retrieving, using, disclosing, restricting, and erasing or destroying it, and there can be risks associated with that processing to the people whose data it is. Failure to adequately protect people's personal information can result in significant, even life-changing harm to some individuals, distress, loss of public trust in us, and legal repercussions including fines and other sanctions.

1.1. Policy purpose

Through this policy we aim to ensure that current and future pupils, staff, volunteers, and other partner organisations can feel confident that our school is a safe and secure place to learn or work, and to demonstrate our commitment to protecting the rights and privacy of everyone whose data we handle by setting out:

- our obligations in the context of what we do;
- clear roles, responsibilities, reporting and management structures aimed at protecting people's personal data and their rights;
- clear procedures for handling data to achieve our aim of taking reasonable and proportionate steps to protect people.

1.2. Policy scope and definitions

This policy applies to all governors, trustees, staff, and volunteers who handle or have access to personal data regardless of where they are physically working e.g. at home, at another organisation, on trips, and to all personal information processed by us or on our behalf. This includes the personal information of our data subjects accessed or used by other organisations which work for or with us e.g. Local Authority workers, contractors, consultants, certain service providers. It may also include the personal data of other people which pupils acquire through schoolwork tasks or while at school e.g. survey results, class Christmas card lists, and pupils will have some responsibilities in line with their capacity to understand and follow rules.

The following definitions explain a little more about our approach to personal data:

'Data processors' are third party organisations which process data on our behalf. They make no decisions about how and why they do that, they just do what we ask them to within the terms of our contract.

'Data subjects' are the people about whom we hold data, and they fall into several general "categories of person", for example, our workforce and their next of kin; pupils, their next of kin, and other

professionals involved with them; our contractors (cleaners, caterers, health & safety, and other service providers); agency and other partner organisation workers (supply or peripatetic teachers, educational psychologists).

'Personal data' is any manually or digitally recorded information relating to a living person (a data subject) which identifies them e.g. a name, an email address, an identification number, location data, an image, an IP address, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person and may include facts or opinions about them. Some of this category of personal data will require enhanced security measures such as encryption, password protection and stricter electronic as well as manual access controls e.g. a locked filing cabinet. This will be determined on the basis of a risk assessment of the harm that failing to secure the data might cause e.g. bank details due to the risk of potential fraud; contact information due to potential harassment etc.

'Sensitive personal data' or **'special category data'** includes disability status, sexual orientation, sex life, ethnicity, medical information (both physical and mental health), political, philosophical and religious opinions/beliefs, trade union membership, and details of criminal convictions or allegations. This category of personal data requires enhanced security measures such as encryption, password protection and stricter electronic as well as manual access controls e.g. a locked filing cabinet.

'Pseudonymised personal or sensitive personal data' is information that has been de-personalised but key-coded and it can fall within the scope of the UK GDPR and this policy depending on how difficult it is to attribute the pseudonym to a particular individual.

'Supervisory Authority' is the body that regulates compliance with the GDPR and in the UK this is the ICO.

'third country' may have two meanings to us.

'Third countries' according to the EU GDPR are states that fall outside of the EU GDPR zone (the EU member states plus Norway, Liechtenstein and Iceland). The EU GDPR restricts transfers of personal data to such 'third countries' unless the personal data is protected in another way, or an exception applies. When the UK left the EU, it became a 'third country' to the EU under EU GDPR and the exceptions that now apply to the UK are the adequacy decision on transfers under EU GDPR and the adequacy decision on transfers under the Law Enforcement Directive on data transfers between the EU and UK.

A 'third country' to the UK after leaving the EU, is any state or country worldwide which is not a part of the UK and to which the UK under UK GDPR restricts transfers of personal data unless the personal data is protected in another way, or an exception applies. The exceptions that currently apply to some of these 'third countries' are limited and described in the adequacy decisions the UK has made (see Section 10.5 for more information).

We will make anyone with whom we share the personal data of our data subjects aware of our relevant policy, procedures, and expectations at the outset of sharing.

Any breach of this policy, or of the Regulation itself must be reported to our Data Protection Officer and may need to be reported to the ICO as the Supervising Authority for the United Kingdom. The breach could be unlawful and result in legal action or prosecution and regardless of any legal repercussions it may also be actionable under our disciplinary procedures.

This policy will be updated as necessary to reflect improving practice in data management, security and control and to ensure compliance with any changes to relevant legislation.

Associated policies or documents include:

- Overarching Safeguarding Statement
- Child Protection Policy and procedures
- Online Safety Policy and procedures
- Freedom of Information Publication Scheme
- Health and Safety Policy and procedures
- Use of Images Policy
- Whole School Behaviour Policy and procedures
- Staff Code of Conduct

2. Roles and Responsibilities

Our responsibilities as a data controller include:

- Analysing and documenting the types of personal data we hold and their uses.
- Identifying our lawful basis for processing personal data.
- Having procedures which support the rights of the individual.
- Ensuring consent procedures are lawful.
- Implementing and reviewing procedures to detect, report, and investigate personal data breaches.
- Storing data in safe and secure ways.
- Assessing risks to individual rights and freedoms should data be compromised.

Staff responsibilities include:

- Understanding their data protection obligations in line with their training and professional duties.
- Checking that their data processing activities comply with our policy and are justified.
- Not using data in any unlawful way.
- Storing data carefully and correctly to avoid breaches of data protection.
- Raising concerns, notifying breaches or errors, and reporting anything suspicious or contradictory to this policy or our legal obligations without delay.

The Data Protection Officer's responsibilities include:

- Keeping governors updated about data protection responsibilities, risks, and issues.
- Reviewing the data protection policy, associated policies, and all relevant procedures regularly.
- Arranging data protection training and advice for all staff and others included in this policy.
- Advising on direct marketing issues such as compliance with the law and our policy; how we deal with queries from target audiences or media outlets; and the wording of data protection statements attached to emails and other marketing copy.
- Answering questions on data protection from staff, governors, and other stakeholders.
- Responding to individuals such as parents, pupils, and employees who want information.
- Checking on and approving of any third parties that handle our data and any contracts or agreements regarding data processing.

The Information Technology Manager's responsibilities include:

- Ensuring all systems, services, software, and equipment meet acceptable security standards and can be appropriately filtered and monitored.
- Checking security hardware and software regularly to ensure it is functioning properly and securely.
- Researching relevant third-party services (cloud services, data shredding etc.) that we are considering using.

3. Data Protection Principles

We understand that as a data controller we are responsible for, and need to be able to demonstrate that we comply with the principles set out in Article 5 of the GDPR which requires that:

a). Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

We aim to achieve this through carefully considering why we need data before we ask people for it; by publishing our Privacy Notices, implementing them, and reminding people about what the notices says when we ask for data; and by educating our workforce on what they mean for their day-to-day practice.

b). Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

By keeping our Privacy Notices updated, implementing them, and educating our workforce about what we have and have not agreed to use data for (also in line with requirement a) above), we can ensure we meet this obligation to restrict our processing of personal data. The law does allow us to further process data for archiving purposes in the public interest, or for scientific or historical

research purposes or statistical purposes and we have declared that we might do this in our Privacy Notice.

c). Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

We will not seek to collect or process personal data which is not strictly necessary for the reasons we asked to be given it. We keep this in mind when we draft data requests and when irrelevant information is provided we take all reasonable steps to return or erase it.

d). Personal data shall be accurate and, where necessary, kept up to date.

We review and update personal data on a regular basis. It is the responsibility of individuals providing personal data to ensure it is accurate. Individuals should notify us by any reasonable means, but preferably in writing, if their personal data needs to be updated e.g. a change of name or contact details. We will take every reasonable step to ensure that inaccurate personal data (after considering the reasons it is being processed), is erased or rectified without delay, for example, some records are historical and should not be changed.

e). Personal data shall be kept for no longer than is necessary.

We will not retain personal data in a form which allows people to be identified for longer than is necessary to use it for the reasons we asked for it. We employ organisational and technical security measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals, as well as follow strict information transfer guidelines when we need to move data e.g. when a pupil leaves to attend another school. We hold regular reviews of the data we retain and destroy or archive it in line with guidance in the '*Information Management Toolkit for Schools*' published by the Information Records Management Society

The law does allow us to retain personal data for archiving purposes in the public interest, or for scientific or historical research purposes or statistical purposes and we have declared that we might do this in our Privacy Notices.

f). Personal data shall be processed in a manner that ensures appropriate security of it.

We understand that our organisational and technical measures to protect data must include protection against unauthorised or unlawful processing and against accidental loss, destruction or damage in the UK, European Union or anywhere else in the world.

We make staff and volunteers aware of their data protection responsibilities and that their duty to preserve confidentiality extends to anywhere that they process the data of our data subjects e.g. at home, on trips etc. and beyond their time of employment with us. See Section 10.2 for more information about the organisational and technological measures we employ to achieve this.

The first principle of data protection is **fair, lawful and transparent processing**, and is the foundation on which everything else is built. We seek to meet the "fair" and "transparent" aspects through our Privacy Notices, and we work hard to ensure that all of the personal data we process meets a condition for lawful processing so that we have a lawful basis to carry it out.

3.1. Conditions for the lawful processing of personal data

To process a piece of personal data we must satisfy at least one condition for the lawful processing of personal data from Article 6 of the GDPR set out in the table below.

6(1)(a)	Consent of the data subject.
6(1)(b)	Necessary for the performance of a contract with the data subject or to take steps to enter into a contract.
6(1)(c)	Necessary for compliance with a legal obligation.
6(1)(d)	Necessary to protect the vital interests (life) of a data subject or another person.
6(1)(e)	Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

6(1)(f)	Necessary for legitimate interests of the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject (not available to processing carried out by public authorities in the performance of their tasks).

We rely on different conditions for the lawful processing of personal data for different things.

To process the personal data of our workforce and volunteers we generally rely on 6(1)(b) i.e. to employ them and provide training, uniform, pay etc. Some pieces of data are processed for other reasons. For example, we use their national insurance number for tax purposes relying on 6(1)(c); we hold their next of kin data relying on 6(1)(d); and we use their image relying on 6(1)(a).

To process the personal data of our pupils we generally rely on 6(1)(e) i.e. to educate them. Some pieces of data are processed for other reasons. For example, we publish their exams results relying on 6(1)(c) because the law requires us to; we hold their next of kin data relying on 6(1)(d); and we use their image sometimes relying on 6(1)(a).

We rely on different conditions to process different pieces of the personal data of families e.g. 6(1)(b) for their financial details to provide meals, photographs etc.; and 6(1)(d) for their contact details in case their child is ill. We use the same criteria to process the personal data of other individuals such as contractors or Local Authority workers etc. where it applies and most often using 6(2)(b) to work together.

3.2. Conditions for the lawful processing of special categories of data

To process a piece of sensitive personal data we must satisfy at least one condition for the lawful processing of special categories of data from Article 9 of the GDPR set out the table below **as well as** one condition from the previous table.

9(2)(a)	Explicit consent of data subject, unless prohibited by EU/National law.
9(2)(b)	Necessary to meet obligations under employment, social security or social protection law, or a collective agreement.
9(2)(c)	Necessary to protect the vital interests (life) of a data subject or another individual where the data subject is physically or legally incapable of consenting.
9(2)(d)	Processing by a not-for-profit body with political, philosophical, religious or trade union aims if it relates only to members/former members (or those in regular contact for those purposes) & there is no disclosure to third parties without consent.
9(2)(e)	Processing relates to personal data already made public by the data subject.
9(2)(f)	For the establishment, exercise or defence of legal claims or court judicial capacity.
9(2)(g)	Substantial public interest under EU/National law proportionate to the aim pursued and which contains appropriate safeguards.
9(2)(h)	For preventative or occupational medicine; assessing work capacity of an employee, medical diagnosis, providing health & social care or treatment or management of healthcare services under EU/National law or contract with a health professional.
9(2)(i)	For public health e.g. protecting against serious cross-border threats to health or ensuring high standards of healthcare & medicinal products or medical devices.

We rely on different conditions for the lawful processing of sensitive personal data for different things.

To process the sensitive personal data of our workforce and volunteers we rely on 9(2)(b) to check their criminal history before employing them; 9(2)(h) to use their health information to protect them at work; 9(2)(a) to share their health information with support services; 9(2)(i) to report on their health to Public Health England (PHE) or the Health & Safety Executive (HSE) as required; and 9(2)(f) to retain accident and ill-health information in case of a claim for compensation.

To process the sensitive personal data of our pupils we rely on 9(2)(b) in respect of child protection and multi-agency safeguarding work; 9(2)(b) or 9(2)(h) to use their health information to protect them at

school; 9(2)(i) to report on their health to PHE or the HSE as required; and 9(2)(f) to retain accident and ill-health information in case of a claim for compensation.

We apply the same criteria to processing the sensitive personal data of families and other individuals such as contractors or Local Authority workers etc. where it applies.

3.3. Deciding which condition to rely on

More than one lawful basis may apply, but we only need **one** basis for each piece of data, and we will rely on what best fits the purpose, not what is easiest. When carrying out a new task or an existing task in a new way, staff should consider the following factors:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are we in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are we able to stop the processing at any time on request, and have we factored in how to do this?

3.4. Privacy Notices

Our Privacy Notices are an important and necessary way of being transparent and telling governors/ trustees, parents, pupils, and staff what we are doing with their information. To comply with the law it will include:

- Our identity and contact details as the data controller and those of our DPO.
- The purpose of the processing and the lawful basis or bases we are relying on.
- Our, or a third party's legitimate interests in having it.
- The categories of personal data we process.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to UK Government determined "third countries" and the safeguards.
- Retention periods or the criteria used to determine them.
- The existence of each of the data subject's rights.
- The right to withdraw consent at any time, where relevant.
- The right to lodge a complaint with the ICO.
- The sources of personal data and whether they are publicly accessible.
- Whether providing personal data is statutory or contractual and the possible consequences of failing to provide it.
- The existence of any automated decision making, including profiling; how decisions are made, the significance and the consequences.

Our privacy notice relevant to pupils can be found at Appendix B, the one relevant to our workforce and volunteers at Appendix C, and the one relevant to our governors at Appendix D. They are also made available on our website, on noticeboards, in communications with parents and staff etc.

4. Individuals' rights and how we protect them

We recognise that all data subjects have "qualified rights" so they are not absolute rights in all circumstances. They are qualified by the rights of other individuals and the legal rights of the data controller or processor to conduct their lawful business.

4.1. The right to be informed about the collection and use of their personal data

Our Privacy Notices seek to provide transparency about our collection of personal data; they are published on our website, pinned to noticeboards, and freely available on request from our office; we

draw people's attention to what they say when we collect data from them; and we regularly review and update the Notices when necessary, particularly if we have changed what we use the data for and before we start using it for the new reason.

4.2. The right of access to their personal data and relevant supplementary information

This includes:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information which largely corresponds to the information we must provide in our Privacy Notices.

Any of our data subjects (or their chosen representative or a person with parental responsibility for them) can make a Subject Access Request (SAR). Please see Section 5 for our procedure on handling SARs.

4.3. The right to rectification if the information held is inaccurate or incomplete

Every individual has a responsibility under UK GDPR to provide accurate data. There is no legal definition of accuracy, but we generally understand it to mean that personal data is inaccurate if it is incorrect or misleading on matters of fact.

The right to rectification will depend on why we asked for the personal data. For example: a person's name should **not** be changed to their new married name on the Single Central Record (SCR) because the SCR is a record of information correct at the time of recruitment and vetting. A note should be added to ensure the SCR record can be matched to the correct living person in case of a vetting query using the married name in future, but the record itself should not be changed.

When we receive a request to change the data we hold, we will take reasonable steps to check that the data is accurate and to rectify it if necessary. This means that the more important it is that the data is accurate, the more effort we will make to correct it. We will take into account arguments and evidence provided by the data subject and anything we have already tried to do to ensure the data is accurate.

We can refuse to comply with a request for rectification if the request is manifestly unfounded or excessive, taking into account whether it is repetitive. We can either request a reasonable fee based on the administrative costs of complying with the request, or we can refuse to deal with the request. We will use ICO guidance and our own information management records to make decisions about this and we will contact the person making the request to inform them of our decision (including any fee payable) and the reasons without undue delay and **within one mon**th. We do not have to comply with the request until we have received the fee.

As a matter of good practice, we will restrict the processing of the personal data in question while we are verifying its accuracy regardless of whether the data subject asked us to as is their right (see Section 4.5).

When we have decided whether the data is accurate or not and whether we will change it or not, we will explain our decision to the individual making the request and inform them of their rights to complain to the ICO. We will also make a record of the request and our response similar to the way we handle SARs e.g. date of receipt, the data subject's name, the name and address of requester *(if different)*, the rectification requested, our decision, and the date we communicated the decision.

4.4. The right to erasure of personal data

Under Article 17 of the GDPR individuals have a new right to have their personal data erased. This is also known as the "right to be forgotten". There are no rules about how a request should be made e.g. verbally, in writing etc. so all staff are trained to recognise someone trying to exercise this right. The right is not absolute and only applies if:

- the personal data is no longer necessary for the reason we originally collected or processed it;
- we are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;
- we are processing the personal data for direct marketing purposes and the individual objects;

- we have processed the personal data unlawfully i.e. in breach of the lawfulness requirement of the 1st principle;
- we have to do it to comply with a legal obligation; or
- we have processed the personal data to offer online "information society services" to a child under the age of 13 e.g. an app, game, social media platform etc. that we subscribe to and offer to children but do not *require* them to use for the purposes of education. Any such services we currently provide or broker are necessary for education purposes so the right to erasure may not apply, but we are aware of our obligations and will act accordingly. We also work hard to appropriately control children's access to the social media platforms we use to communicate with our community.

We have to give special consideration to any request for erasure if the processing of the data is solely based on consent given by a child, especially any processing of their personal data (usually images) on the internet. This is still the case when the data subject is no longer a child because a child may not have been fully aware of the risks involved in the processing at the time of consent. In some circumstances we might need to give more weight to a request for erasure from a child if their parent has already consented to the use of their data e.g. removing pictures from our school website when a parent has consented but the child whose images they are objects. We will need to do this if we are confident that the child understands their rights and the effects on them of their request. For more information about how we decide whether a child understands please see Section 5 on Subject Access Requests.

Unless it is impossible or disproportionate, we have to tell other organisations about erased data if:

- the personal data we erased has been disclosed by us to others; or
- the personal data has been made public in an online environment (for example on social networks, forums or websites).

If we are asked, we should also tell the individual about the other organisations we gave their data to.

The right to erasure does **not** apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to make achievement of that processing impossible or disproportionately difficult; or
- for the establishment, exercise or defence of legal claims.

There are also two circumstances when the right to erasure does **not** apply to special category data:

- if the processing is necessary for public health purposes in the public interest; or
- if the processing is necessary for the purposes of preventative or occupational medicine.

When we receive a request to erase data, we will take reasonable steps to check the identity of the requester and that they have the right to make the request before considering it.

We can refuse to comply with a request when an exemption applies, or when the request is manifestly unfounded or excessive. We can either request a reasonable fee based on the administrative costs of complying with the request, or we can refuse to deal with the request. We will use ICO guidance and our own information management records to make decisions about this and we will contact the person making the request to inform them of our decision (including any fee payable) and the reasons without undue delay and **within one month**. We do not have to comply with the request until we have received the fee.

When we have decided whether we can erase the data we will explain our decision to the individual making the request and inform them of their rights to complain to the ICO. We will also make a record of the request and our response similar to the way we handle SARs e.g. date and manner of request (verbally to class teacher, a note handed to reception etc.), the data subject's name, the name and address of requester *(if different)*, the erasure requested, our decision, and the date we communicated the decision.

4.5. The right to restrict the processing of personal data

Under Article 18 of the GDPR individuals have the right to limit the way we use their data if they have a particular reason for wanting to, and this is an alternative to erasing it. They may have issues with the content of the information or how we have processed it. In most cases we will not be required to restrict an individual's personal data indefinitely but will need to have the restriction in place for a certain period of time. The right is not absolute and only applies if:

- the individual contests the accuracy of their personal data and we are verifying it;
- the data has been unlawfully processed i.e. in breach of the 1st principle, and the individual doesn't want it erased;
- we no longer need the personal data but the individual needs us to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to us processing their data under Article 21(1), and we are considering whether our legitimate grounds override those of the individual.

We use the most appropriate method applicable at the time to restrict processing including:

- temporarily moving the data to another processing system;
- making the data unavailable to users; or
- temporarily removing published data from a website.

While a restriction is in place we will not do anything with data except store it unless:

- we have the individual's consent;
- it is for the establishment, exercise or defence of legal claims;
- it is for the protection of the rights of another person; or
- it is for reasons of important public interest.

If we have disclosed the restricted data to another organisation we will tell them about the restriction in the same way as if it were inaccurate data unless this proves impossible or involves disproportionate effort. If asked to, we will also inform the individual about these recipients.

We can lift the restriction when we have decided that the issues are resolved i.e. the data is accurate or our legitimate grounds override the individuals' and we will inform the individual and include our reasons before we lift it. We will also tell them about their right to make a complaint to the ICO.

We can refuse to comply with a request when the request is manifestly unfounded or excessive. We can either request a reasonable fee based on the administrative costs of complying with the request, or we can refuse to deal with the request. We will use ICO guidance and our own information management records to make decisions about this and we will contact the person making the request to inform them of our decision (including any fee payable) and the reasons without undue delay. We do not have to comply with the request until we have received the fee.

4.6. The right to data portability

The right to data portability only applies when all 3 of the following conditions are met:

- the individual has provided the personal data;
- the processing is based on the individual's consent or for performance of a contract; **and**
- processing is carried out by automated means.

We do not currently hold any qualifying data, but we are aware of our legal obligations and will follow ICO guidance, reviewing our procedures if we automate any processing.

4.7. The right to object to processing

Individuals must have an objection on "grounds relating to his or her particular situation" and we must stop processing the personal data unless:

- we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

We will:

- inform individuals of their right to object "at the point of first communication" and in our privacy notices, explicitly bringing the right to their attention clearly and separately from any other information;
- stop processing personal data for *direct marketing purposes* as soon as we receive an objection because there are no exemptions or grounds to refuse; and
- deal with an objection to processing for *direct marketing* at any time and free of charge.

An individual can object to processing for research purposes on "grounds relating to his or her particular situation" unless processing is necessary for the performance of a public interest task.

We carry out some processing of personal data securely in encrypted online systems e.g. our visits approval system, responding to DfE data demands online, and any individual can object to our online processing by contacting us at info@kksa.co.uk.

4.8. The right to object to automated decision making and profiling

We do not currently use any data systems that make automatic decisions about people without any human involvement. We are aware of our legal obligations and will follow ICO guidance, reviewing our policy and procedures if we fully automate any decision-making.

5. Subject Access Requests

Every individual who is our data subject has the right to access their personal data so that they are aware of and can verify the lawfulness of the processing, including children of any age who understand what they are requesting. These rights do not automatically override the rights of any other individual who might be identified by our response to a request, so we will make a decision on what information to disclose by balancing the data subject's right of access against any other individuals' rights in respect of their own personal data. We will use the latest ICO guidance on SARs to help us make decisions.

The data subject or the person acting on their behalf must make a SAR in writing and we provide a form at Appendix A to help people do this. There is no requirement to use our form, but it can speed up the process by helping the people making requests to provide us with the kind of information we need to comply. We will also make any reasonable adjustment for disabled people who may be unable to make their SAR or receive information in writing e.g. accepting a verbal request, providing a braille response etc. Relevant staff are trained to recognise a SAR even when it does not include the words "subject access", or refer to the applicable legislation, including where the wrong legislation is quoted i.e. often the Freedom of Information Act.

When we receive a SAR it will be entered in the Subject Access Request log book, including the date of receipt, the data subject's name, the name and address of requester *(if different)*, the type of data requested (e.g. pupil record, personnel record), whether there is enough information to respond appropriately (and the immediate action taken to seek more if not), and the expected date for providing the information.

We aim to provide information without delay and at the latest **within one month** of receipt of the request. For example: if we receive a SAR on the 10th of the month we will respond by the 10th of the following month. We will seek to extend this response period by up to the two further months which the law allows where requests are complex or numerous. If this is the case, we will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

SARs made by pupils will be processed in the same way as any other SAR and the information will be provided to the child regardless of their age unless it is clear that they do not understand their rights. If we are sure that the pupil **does not** understand the SAR and their rights, we will refer the matter to parents, comply if they agree, and provide the information to parents.

SARs made by people on behalf of children they hold parental responsibility for will be processed in the same way as any other SAR while recognising that they do not own the data they are requesting. If we are confident that the pupil whose data it is **does** understand the SAR and their rights, then we will respond to the child rather than the parent, even where the parent was the one who made the request.

In making our decision we will take the following, amongst other things, into account:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person (including information about any counselling or other service being offered directly to the child);
- any consequences of allowing those with parental responsibility access to the child's or young person's information (particularly important if there have been allegations of abuse or ill treatment);
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

If the information requested by a parent in a SAR relates to the 'educational record' of a pupil, in accordance with *'The Education (Pupil Information) (England) Regulations 2005'*, we will make a pupil's educational record available for inspection by the parent, free of charge, **within fifteen school days** of receipt of the parent's written request for access. This cannot include any information that we could not lawfully disclose to the pupil themselves. If parents request a copy to keep, we can charge the administrative costs of supplying one.

If the information requested in a SAR does **not** relate to the 'educational record' of a pupil, we will provide a copy of the information free of charge **unless** the request is manifestly unfounded or excessive, particularly if it is repetitive. This fee may vary and will be based only on the administrative cost of providing the information. We will use ICO guidance and our own information management records to make decisions about this.

We must verify the identity of the person making the request, using "reasonable means". If the person making the request is not the data subject, we must also verify their right to make such requests on behalf of the data subject e.g. their authority to act or their parental responsibility for a child. In cases where a child is competent to make their own request, information will be provided to the child and not to the parent. We will use ICO guidance and our knowledge of the capability of our pupils as described above to make decisions about this.

If the request is made electronically, we will provide the information in a commonly used electronic format.

If we are asked for a large quantity of information about an individual, we can ask the individual to be more specific about the information they want. This is not because we are exempt from providing large amounts of data, this is so we can consider whether the request is manifestly unfounded or excessive.

If we are asked for information that a data processor we work with holds on our behalf, we will ask our data processor to provide it to us so that we can comply with the SAR. This is because we are the data controller and it is our responsibility. We have written contracts in place with all of our data processors to help us do this.

A Subject Access Request should be made in writing to: Lesley Blamire at info@kksa.co.uk.

6. Data Protection and Privacy by Design

Data protection and privacy by design is an approach to projects and tasks that promotes privacy and data protection compliance from the start and is a clear legal requirement of us. This is not just about the strategic decisions we make building new IT systems for storing or accessing personal data and developing policy or strategies that have privacy implications. It is also about collecting or sharing data in a new way or using data for new purposes.

Our aim is to minimise privacy risks and build trust so all staff will have a central role to play in keeping what we do compliant. When handling data in a different way staff are trained to first consider the impact of what they are doing and how they are doing it in relation to data protection and privacy, with the ten questions in Section 3.3 playing an important part in the process. This could be as simple as ensuring consent forms containing sensitive personal data are not carried in a clear folder on a trip, or as

complex as thoroughly vetting an overseas data transfer service when a pupil leaves us to attend a school outside the European Economic Area (EEA).

We use the ICO guidance on Data Protection Impact Assessments (DPIAs) as an integral part of our approach to data protection and privacy by design. We also consult our DPO at the outset of any new data project.

6.1. DPIAs

We understand that we have a legal obligation to do a Data Protection Impact Assessment (DPIA) before carrying out processing likely to result in a high risk to individuals' interests. If our DPIA identifies a high risk which we cannot mitigate, we must consult the ICO before proceeding.

A DPIA is a process to systematically analyse our processing and help us identify and minimise data protection risks. It is meant to:

- describe the processing and our purposes;
- assess the necessity and proportionality of what we are planning;
- identify and assess risks to individuals; and
- identify any measures to mitigate those risks and protect the data.

It does not have to eradicate the risk but should help to minimise risks and consider whether or not they are justified. We will need to do a DPIA if we plan to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric or genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

All staff have a responsibility to identify when their activities around data imply the need for a DPIA. This could be doing an entirely new task with data, or it could be changing the way a well-established task is being done. Amanda Eastwood, our Data Protection Officer is responsible for conducting DPIAs.

Training & Awareness

During their induction, all staff and volunteers will receive suitable training in their responsibilities for data protection in their work or volunteering, and the relevant procedures. This will be supplemented with staff briefings, inset training, and other methods of updating staff and volunteers as necessary e.g. briefing emails, notices etc.

This policy is available to all staff and volunteers in hard copy in the School Reception and electronically on the staff network (Google Drive/Shared Drives/Staff Area/Policies & Procedures). It can also be provided to others on request. This policy will be updated regularly in line with changes in practice or clarifications required after applying it to resolve data protection issues.

Anyone can seek general data handling guidance from the ICO on their website https://ico.org.uk.

Day-to-day support and guidance for staff is available Amanda Eastwood, our Data Protection Officer. Any other category of person wanting help with a data protection issue e.g. contractors, parents etc. can also contact Amanda Eastwood, our Data Protection Officer.

7. Publication of Information

At times we publish information which includes personal data, for example:

- internal telephone directory,

- event information,
- staff information,
- lists of students in a team.

Other things we publish can be subject to an individual's consent and we will seek it as required and consider all reasonable requests to correct, erase or restrict data processing in line with our legal obligations.

8. Managing Consent

We only need one lawful reason to process personal and special category data and the law provides us with 6 reasons to choose from for personal data (see Section 3.1) and 9 reasons for sensitive personal data (see Section 3.2). This means it is extremely rare for us to have to rely solely on consent as our *only* lawful basis for processing.

When we do need consent and we ask for it, we will include the following information in our request:

- the name of our school;
- the name of any third party controllers who will rely on the consent;
- why we want the data;
- what we will do with it; and
- that individuals can withdraw consent at any time.

People will be asked to actively indicate their consent in words and if there are different options, these will be made clear e.g. consent for a child to participate in an event being clearly separate from any consent to use images of them taken at the event (if no standing images consent is already held).

There is no set time limit for consent. How long it lasts depends on the context and what we have told people in our Privacy Notices or other communications. We review and refresh consents as appropriate.

Genuine consent should put individuals in control, build trust and engagement, and enhance our reputation so, when we do rely on it, we need to keep a record that helps show it was freely given e.g. who consented, when, how, and what they were told.

8.1. Consent to use personal data including images and voice recordings

We *do not* need parental consent to process any personal data including image or voice recordings for the purposes of education e.g photographs or video of a student completing their PE Practical Assessment for their GSCE examination Using names, image and voice recordings of children in their work and in displays inside school, is a fundamental part of their education, personal development and how we celebrate them. This does not affect the statutory rights of individuals as set out in Section 4. Anyone can raise any concern with any member of staff about our use of their or their child's data at any time and we are obliged to ensure their rights are upheld where we have no lawful reason to refuse.

We *do* need parental consent to use personal data including image and voice recordings for other reasons such as marketing or self-promotion in publications and on websites or social media platforms directly managed by us or, with our permission, by others associated with us and may include pictures that have been drawn by children. Images that might cause embarrassment or distress will not be used nor will image or voice recordings of children be associated with materials or issues that are considered sensitive. Anyone with parental responsibility for a child can ask to see any images that we hold of them at any time.

There is no legally binding age of consent in the UK with regard to the use of an individual's own data, including their image or voice, except when providing an Information Society Service (ISS) directly to a child online and solely on the basis of their consent. In the UK this particular age of consent is 13 years old. We do not currently offer any ISS and have no plans to. This means that any child of any age can assert their data rights or consent to the use of their data under the law, providing we are sure that they understand their rights and the implications of their consent. For more information about how we make decisions about a child's competence to consent or withdraw consent that their parents have previously provided, please see Section 5.

Photography, audio recording or filming will only take place at school or school events with the permission of the Head teacher/ manager, and under appropriate supervision.

Regardless of who is publishing data, and that includes us, our policy is that children will only be named if there is a particular reason to do so e.g. they have won a prize, and no other personal details will be published or given out. If names will, or might, be published e.g. in a newspaper article, we will check that parents understand the potential implications and consent to the use of names at that time and before the publishing happens. The news media will often require a child's full name before they will publish an image and our policy is to resist this wherever possible and if we fail, we will take steps to ensure that parents are aware that all of the details will be available in local or national newspapers and worldwide online.

We allow parents, carers, and other invited visitors to take images of children at school functions, but we reserve the right to enforce special restrictions on a case-by-case basis. They are required to bear in mind that they may capture other people's children and must ensure images are appropriate. They are also required to agree that they will only share them publicly i.e. post them to social media, with the express permission of the parents of everyone in the images. In our Behaviour Policy and our Online Safety Policy we also require all parents and children to support our approach to online safety and not upload or post to the internet any pictures, audio, video or text that could upset, offend or threaten the safety of any member of the school community or bring the school into disrepute.

Our policy around consent is to ask once when a child starts their career with us for separate general consents to use image and/or voice recordings:

a) publishing on our website or in other print or online media which we directly control, or
b) allowing carefully selected third party organisations such as local media outlets to publish them.

We use the form at Appendix E to seek consent and we remind parents and children regularly that they can change or withdraw their consent at any time.

When a child understands their right of consent and its full effects and there are no reasons why their name, image or voice must be protected, we can prioritise the consent of a child over parental consent where they are different. We are more likely to decide not to use images etc. when a child objects and their parent does not than vice versa, but our overriding priority will always be to act in the child's best interests.

Staff are expected to make themselves aware of any guidance we use from our local authority, Local Safeguarding Children Partnership, or governors, or KAHSC General Safety Series G21: The Use of Images Working with Children, and to apply the principles in all use of image and voice recordings.

8.2. Data sharing during a public health emergency: consent and data retention

In line with our statutory duties, we require anyone who comes into close contact with our pupils. staff, buildings, or equipment (including our staff and pupils) to share with us necessary personal data to give to an organisation authorised by a relevant public health authority so they can take action to protect public health. We do not need consent for this and in a public health emergency this is no different to our normal practice when we are required to report that staff or pupils have contracted a notifiable disease like meningitis or measles, or if we have a food poisoning incident on our premises.

9. Data Security and Integrity

Article 5(1)(f) of the GDPR concerns the 'integrity and confidentiality' of personal data. It says that personal data shall be: "Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

The security measures we put in place seek to ensure that the data:

- can be accessed, altered, disclosed or deleted only by those we have authorised to do so and that those people only act within the scope of the authority we give them;
- is accurate and complete in relation to why we are processing it; and

- remains accessible and usable, i.e. if personal data is accidentally lost, altered or destroyed, we should be able to recover it and prevent any damage or distress to individuals.

All staff and any others who process the personal data of our data subjects are expected to work to the same principles we do at all times.

9.1. Classification of data

We carry out regular data audits to identify data that we control and the risks to every kind of processing we do to that data, and we keep a record to help us deal with any issues or requests. As part of this systematic approach we operate 3 levels of data classification to ensure the appropriate security measures can be taken to keep the data safe:

- **Public:** Information that does not require protection and is considered "open and unclassified" and which may be seen by anyone whether directly linked with school or not. Information is likely to already exist in the public domain e.g. the information the DfE publishes about our governors on the Get Information About Schools public database online.
- **Confidential:** Information that, if disclosed inappropriately, may result in minor reputational or financial damage to the school or may result in a minor privacy breach for an individual. Information that should only be available to sub-groups of school staff who need the information to carry out their roles.
- **Sensitive:** Information that has the potential to cause serious damage or distress to individuals or serious damage to the school's interests if disclosed inappropriately. Information which is sensitive in some way because it might be sensitive personal data, commercially sensitive, legally privileged or under embargo. This information should only be available to a small tightly restricted group of authorised users.

The appropriate marking of data as to its classification is an operational decision on a case-by-case basis. Most of our data held in electronic databases is classified automatically by the information management systems that hold it. Information that is transferred e.g. emailed, posted, moved to an archive etc. must be appropriate classified and marked to ensure it will be treated properly.

Appendix H sets out some of our specific data security expectations at each different level of data classification and we share it with staff and others who have legal obligation to us when they process data that we control.

All data classifications are reviewed at the point of entry into our archive. All archived data is appropriately labelled with:

- the final data classification;
- any specific restrictions i.e. not to be released to named parent under court order;
- how the data is to be destroyed e.g. incineration, cross-cut shredding, shredding, or electronic data scrubbing/shredding;
- when the data is to be destroyed.

Staff responsible for archiving are trained to assess and manage any increasing risks that can arise as data about one person is aggregated.

9.2. Organisational and technical security measures

The main organisational and technical measures we employ include:

- Appropriate physical security measures for the site, buildings, restricted areas and restricted storage containers including locks, deadlocks, restricted access codes, alarms, window bars, and computer hardware cable locks.
- Appropriate physical access and security procedures including limiting access to areas or stores to certain key holders, and procedures to welcome visitors aimed at preventing unauthorised access e.g. visitors' badges, signing in/out, whether a visitor can only access certain areas while accompanied etc.
- Ensuring unauthorised personnel cannot see documents or screens which might display personal data e.g. open registers and visitor's books, emails, CCTV monitors.

- Suitable contracts of employment or technology access agreements for pupils, visitors and others aimed at ensuring the proper use of personal data and maintenance of confidentiality.
- Appropriate storage arrangements that avoid physical risks (flood, fire etc.), loss (lost devices, accidental destruction etc.) or electronic degradation (corruption caused by electricity or magnetism, new software unable to read files created using old software etc.).
- Appropriate technological or procedural security measures including:
    - The installation of appropriate security software (including for virus and malware checking) on all devices used to process personal data, instructions on how to use it properly, and the requirement on all data users to adequately secure devices i.e. carrying portable devices securely and activating an encrypted screen lock when leaving a device unattended even for a minute.
    - Restricting access to school devices containing personal data to employees and specially authorised volunteers, visitors or service providers. Staff using a work device off-site must take steps to secure their work device from use by anyone else including family.
    - Enforcing our strict protocol on the use of personal devices to process personal data obtained at work, including a requirement for secure remote access to school systems.
    - Restricting the number of people who can access certain data by limiting online logins, protecting parts of our network to hide them from unauthorised users, and by having procedures in place to designate authorised users and give only them the proper access;
    - Enforcing our strict password protocol for access to any personal data whether it is online, on a device, or being transferred somewhere e.g. email. All staff who use Password Managers are required to apply the best practice guidance blog from the National Cyber Security Centre (NCSC).
    - Having appropriate data recovery arrangements in place to avoid accidental loss of data or password sharing i.e. so when someone is unavailable to provide access to data, with the proper authorisation their access can be reset and the data still obtained in their absence.
    - Appropriate marking or designating of data as private or confidential or sensitive to ensure it is treated accordingly e.g. not printed to a publicly accessible printer.
    - Adherence to strict controls on the transfer of data i.e. only as authorised and agreed via encrypted email or portable device, secure websites, password protected files, properly addressed and if necessary fully tracked postal packages, delivery by hand etc.
    - Secure methods of disposal for both paper and electronic data shredding.
    - Clear policies and procedures for the appropriate archiving and automatic backing up of necessary data including off-site e.g. essential data identified in the Emergency Preparedness Plan to ensure business continuity.
    - Clear and binding contracts with our data processors such as our health & safety provider and people who we jointly control data with such as the outdoor adventure centres we go on residential trips to.

All enquiries about the policies and procedures that should be followed and how data should be protected or destroyed can be addressed to the DPO or the IT Manager.

The consequences of getting data security wrong can be very serious for our most vulnerable data subjects and breaches of data protection may be subject to disciplinary action and further subject to legal action or criminal prosecution.

9.3. Email

All staff are expected to adhere to the good practice around the use of email set out in the current Information and Records Management Society *'Toolkit for Schools'* understanding their role and responsibilities with regard to:

- the 8 things they must know about email including that it is not always a secure medium to send confidential information by, that email is disclosable under the Freedom of Information Act 2000, that any employer has a right to monitor the use of email under the Regulation of Investigatory Powers Act 2000, and that email is one of the most common causes of stress in the work-place;
- creating and sending email;
- sending attachments;
- using disclaimers;

- managing received e-mails; and
- retaining emails.

Others who have legal obligations to us because they process data we control will be made aware of our email protocols as necessary.

All staff are required to use the authorised email disclaimer as follows:

> *The information contained in this e-mail communication may be confidential. If you are not the intended recipient, or have received this message in error, please notify the sender and then destroy any electronic or paper copy of this message.*

9.4. CCTV

We use CCTV to monitor and record images for the purposes of crime prevention and public safety both inside and outside our buildings. Coverage is designed to minimise any intrusion on reasonable expectations of privacy and we have clear procedures governing the use, retention and disclosure of the personal data we capture which are appended to this Policy.

9.5. Transfers of data outside the UK

Transfers of personal data outside the UK are treated differently depending on which countries it is being transferred between or through, what is being transferred, why and how, and how closely those countries' approaches to data protection align with the UK's.

We will follow current ICO guidance on International transfers after the UK exit from the EU Implementation Period and Standard Contractual Clauses (SCCs) after the transition period ends for country specific requirements when we need to transfer personal data internationally.

Regarding transfers between the UK and the EU:

When the UK left the EU on 31 January 2020 it entered a "transition" period which kept existing UK-EU data transfer rules aligned as if the UK were still part of the EU ('frozen GDPR'). This allowed freedom of movement for data to continue to flow as before.

On 28 June 2021, the EU approved adequacy decisions for the EU GDPR and the Law Enforcement Directive (LED) i.e. it was agreed that the UK as a third country to the EU ensures an adequate level of protection of the rights and freedoms of EU data subjects to allow transfers. This means that data (excluding data transferred from the EU to the UK for the purposes of UK immigration control) can continue to flow as it did before, in the majority of circumstances until 27 June 2025.

Following the above ICO guidance allows us to continue to meet our data protection obligations. We will also refer new or uncertain international transfers of personal data to or from the UK to our DPO when making decisions about the safety, security, and lawfulness of transferring it.

9.6. Record keeping

The legislation contains some explicit provisions about documenting our processing activities but that is not the reason we keep records. We need to know what data we have and how we use it to be able to control it effectively; we need to be able to justify our decisions about data; and we may need to provide evidence to the ICO as part of a data breach investigation.

We use the ICO GDPR Documentation Template to fully comply with the record keeping required of us under Article 30. It is the responsibility of all staff to ensure the spreadsheet remains a current reflection of how they work with data.

We also keep records of our DPIAs, consent, staff training, and our contracts and data sharing agreements i.e. our employment and service provision contracts, processor contracts, and joint-controller data sharing agreements.

We also keep some simple logs which briefly detail:

- SARs;

- other types of data requests and what we did e.g. objection, rectification, withdrawal of consent, education record request etc.;
- data destruction;
- breaches.

All staff are made aware of our record keeping obligations and some staff are specially trained in managing them.

10. Data Sharing

We are required to share personal data with some organisations by law e.g. our census data with the DfE. At other times we share information to improve or protect people's lives and we have included information about this in our Privacy Notices.

All staff are expected to make reference to the current ICO Data Sharing Checklist in making decisions on whether to share data or not and how to do it. Unless the data sharing is routine and pre-authorised e.g. medical data routinely disclosed to the outdoor adventure centres we go on residential trips to, no decision should be made regarding the disclosure of any sensitive personal or sensitive commercial data without reference to an immediate line manager or the headteacher. If nobody involved in the decision-making has received suitable training in data protection, the DPO must be consulted before data is disclosed externally.

With regard to the disclosure of child protection data, we will always follow the current *'Information Sharing Protocol'* available from our Local Children's Safeguarding Partnership.

We have simple procedures in place regarding unavoidable disclosures to people we do not already have data processing or data sharing agreements with e.g. to an engineer during emergency repair of a computer system, which includes a requirement for them to sign a suitable non-disclosure agreement.

11. Data Retention

We can only keep personal data for as long as we need it. How long that is will depend on the circumstances and the reasons we obtained it.

We will generally follow the guidelines set out in the current Information and Records Management Society *'Toolkit for Schools'*, Local Authority and Local Children's Safeguarding Partnership in particular.

We typically retain pupil data and data about their family and other involved professionals until they leave us. Otherwise we retain it for a few days or weeks e.g. trip consent forms, or for 3-50 years depending on whether it is education related or incident related.

We typically retain workforce data for between 6 months and 6 years after an event or the end of their employment with us, depending on their role. Some pieces of data may need to be retained for 50 years such as records of potential exposure to radiation or asbestos.

We typically retain the personal data of contractors and other professionals in line with work done or contractual agreements, and longer in cases of dispute.

Some information is retained for more indefinite periods e.g. outreach programme take-up data so that we can analyse trends, or event photographs and accounts so that we can maintain a historical record.

We are required to keep indefinitely all child protection information that does not automatically move with a child and remain live information elsewhere when they leave us, pending the outcome of the Independent Inquiry into Child Sexual Abuse.

12. Data Disposal

We will dispose of all paper and digital data securely when it is no longer required.

A Destruction Log will be kept of all data that is disposed of. The log will include any document ID, classification, date of destruction, method and authorisation.

13. Breach Reporting

Any breach of this policy or of data protection laws must be reported to the DPO as soon as practically possible i.e. as soon it becomes apparent. We have a legal obligation to report any qualifying data breaches to the ICO within 72 hours.

A qualifying data breach is one where, if not addressed in an appropriate and timely manner, it could result in physical, material or non-material damage to someone such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to them.

If we experience a data breach and we are unsure whether it is a qualifying data breach that must be reported to the ICO, we will use the ICO self-assessment tool to decide.

All staff and anyone else who owes us or our data subjects a legal duty, a duty of care, or a duty of confidentiality have an obligation to report actual or potential data protection compliance failures. This allows us to:

- investigate the failure and take remedial steps if necessary;
- maintain a register of compliance failures;
- notify the individuals affected; and
- notify the ICO of any compliance failures that are material in their own right or part of a pattern of failures.

Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures may be liable to disciplinary action. Where others have been involved in a data breach, a report will also be made to their employer or DPO if relevant to the breach.

14. Our Obligations to our Data Processors

As the data controller we have obligations to our data processors when we give them the personal data of our data subjects which include in general, but are not limited to responsibilities to:

- provide accurate personal data and all necessary corrections in a timely manner;
- employ appropriate technical and organisational security measures when providing and using the personal data being processed;
- only request user access to the data processing for employees and the contractor at a level commensurate with their work tasks and responsibilities e.g. have the fewest possible users who are authorised and enabled to access the accident & incident reporting system which contains sensitive health data;
- respond promptly to requests from our processors for data updates and provide updated and accurate written instruction regarding the continued access to data that we require;
- require our users of any data processor's system to comply with strict password security measures e.g. length, complexity, not shared etc.;
- take appropriate action regarding any breaches;
- ensure our users of a processor's system website understand their responsibilities with regard to the DPA and the GDPR. Anyone found to have carried out unauthorised or unlawful processing activities must be made aware that they will be subject to disciplinary action by you and may be further subject to legal action or prosecution.
- inform our processor as immediately as possible if:
    - we need to remove security access i.e. to our data on their system, from individuals who no longer have any legal right or authority to access it e.g. employees who have left our employment,
    - we need their assistance to comply with a Subject Access Request,
    - we need them to stop processing the personal data of any of our data subjects,

- be sure of our grounds under the law for asking a processor to stop processing the personal data of any of our data subjects and that they are compatible with other applicable laws or legal rights,
- be very sure of our grounds to erase data under the law because we can expect to pay the full costs of any extraordinary measures required to recover erased data where we have failed in our duties.

All staff involved in using the data that we control with the processing services that we contract with have a duty to meet all of our conditions of service. Queries about our contracts for processing activities should be addressed to: David Finch, IT Manager.

Appendix A

Kirkbie Kendal School
Subject Access Request (SAR) Form

Under the Data Protection Act 2018 you have the right to ask us to supply you with a copy of any personal data we hold about you. This form is provided to help you give us the information we need to deal with your request. You do not have to use it but doing so will make it easier for us to respond fully and quickly.

Information supplied in this form will only be used for the purposes of identifying the personal data you are asking for and responding to your request. It will be processed in line with our data protection policy available from the school office or school website www.kirkbiekendalschool.cumbria.sch.uk

If you want information about the categories of personal data we collect, our lawful bases for processing it, who we share it with and why, how long we keep it for, and your rights, please see our Privacy Notices available from the school office or school website www.kirkbiekendalschool.cumbria.sch.uk

You can complete this form to make a SAR on behalf of someone else (acting as a third party) with their consent.

We aim to respond promptly and within one month of the date we receive your completed SAR form (or request that we recognise as a SAR) *or* the date we receive any further information that we need before we can comply with your request. If we consider your request complex, we can take up to an additional two months to respond. If this is the case, we will let you know within the one-month deadline, and as soon as possible.

We may consider your request complex if it:

- involves retrieval and appraisal of information from multiple sources;
- involves the retrieval of large volumes of information for one data subject which are difficult to separate from information relating to other data subjects;
- is one in a series of requests from the same person;
- involves the release of third-party data for which consent has been refused or cannot be obtained.

For the majority of cases, there is no fee to pay to make this request. However, if the request is deemed excessive or is a manifestly unfounded or repeat request, we may contact you to discuss an appropriate charge.

Before we can process a SAR for:

- Your own personal data, we need to see proof of your identity and address to satisfy us that you are the person legally entitled to have it.
- The personal data of a child you hold parental responsibility for, we need to see proof of your identity and address and proof of your parental responsibility to satisfy us that you are the person legally entitled to have it.
- The personal data of someone else who has asked you to make a request on their behalf as a third-party, we need to see proof of your identity and address, proof of the data subject's identity and address, and proof that the data subject has consented to you making this request for them.

Proof of identity and address in one document can be found on a photocard Driver's Licence.

Other proofs of identity include a current passport (photo page), current national identity card, birth certificate.

Proofs of address must be dated within the last 3 months and could include a bank statement, credit card statement, utility bill, council tax statement, TV licence, HMRC tax document.

Proofs of parental responsibility could include a copy of (please do not include original documents):

Birth mothers (married or unmarried to the birth father) - child's birth certificate naming the child and mother.

Birth fathers (married to the birth mother) - child's birth certificate naming the child and father and the parents' marriage certificate.

Birth fathers (children born after 1 December 2003 when unmarried to the birth mother) - child's birth certificate showing re-registration of the birth after 1 December 2003 and naming the birth father, or a court order e.g. Parental Responsibility Order, or Residence Order, or proof of being appointed the child's Guardian by a Court, by the child's birth mother or by another Guardian, or a Parental Responsibility Agreement with the birth mother.

Birth fathers (children born before 1 December 2003 when unmarried to the birth mother) - child's birth certificate showing re-registration of the birth after 1 December 2003 or any document as for children born before 2003 above.

A person who is not the parent of a child aged 15 or under - a court order like a Residence or Special Guardianship Order, or proof of permission to make the SAR e.g. a signed letter of consent from a person with parental responsibility and/or from the child (if the child is aged 13 or over).

An adoptive parent of a child aged 15 or under - the Adoption Order. For all initial queries about a SAR, please contact Lesley Blamire at info@kksa.co.uk.

We reserve the right to refuse your request if we are not satisfied you are who you claim to be or if we are unsure whether you have the legal right or valid consent from the data subject to make the request.

Section 1: Subject Access Request Declaration

I am the data subject (the person the information is about): ☐ (Complete Section **2** onwards)
I am acting on behalf of the data subject: ☐ (Complete Section **1a** onwards)

Section 1a: Requestor's Personal Details

Surname: ..... Full Forename(s): .....

My relationship to the data subject is: .....

Children aged 13 or over should make their own SAR unless they do not understand the request.

If you are acting on behalf of a child for whom you have parental responsibility, the child will be asked to consent to the information being released regardless of their age where they have the mental capacity to understand the request:

The child is aged 12 or under so obtaining consent independently of parents or carers may not be appropriate ☐
The child is aged 13-15 and needs to complete a consent slip independently of parents or carers ☐
The young person is aged 16 or 17 and has written and signed a letter of consent (please attach) ☐

If you are acting as a third party on behalf of a data subject:

The data subject has provided consent to disclose the information requested YES ☐ (please attach) NO ☐

Address (if different from the data subject's): .....

.....

Tel. number: ..... Email address: .....

Section 2: Data Subject's Personal Details

Surname: ..... Full Forename(s): .....

Date of Birth: ..... Class or job role: .....

Address: .....

.....

Tel. number: ..... Email address: .....

Section 3: Details of the Subject Access Request

Please provide as much information as possible to help us find the personal data you want e.g. relevant dates or names, or if you believe a particular person or department holds the information, please tell us. *Please note* you are only entitled to personal data about the data subject and not third-party data (information about other people).

Section 4: Proof of Identity, Address, Parental Responsibility, Other Legal Right, and Consent

A person making a SAR must show they have the legal right to do so i.e. that they are the data subject, or they have parental responsibility for the data subject and/or have written consent from them. Data will not be disclosed without proof of identity for the data subject *and* the requestor if different *and* any written consent necessary.
Please list the documents you are providing copies of as proof (see overleaf - please *do not* provide original documents).

Section 5: Data Subject Declaration

I declare that to the best of my knowledge the information I have provided on this form is correct.

Signature of data subject (or parent/carer of): ..... **Date:** .....

Name of data subject (or parent/carer of) **Please print:** .....

Appendix B

Student Privacy Notice
(How we use student information)

What's this about?

A new law was introduced in 2018 that helps keeps your information safe – things like your address, date of birth and phone number. The school and other people collect and use information for all kinds of reasons, and the new law tells them exactly what they are allowed to do with your information.

We collect some information about our students, like you. It's our job to tell you how we will collect the information, how we will record it and how we will use it.

In this notice, you will see different names or terms used that you may not be familiar with, such as:

- **Data controller**: This person (or group of people, like a school) is in charge of the information we collect.
- **Data processor**: This person processes information for the data controller.
- **Data protection officer** (DPO): This person makes sure we do everything the law says. The school's DPO is Mrs Eastwood.
- **Personal data**: This means any information that can be used to identify someone, such as your address and date of birth.

Who looks after your information?

The school is the data controller of the personal information you give us – we look at how and why your information is collected and used.

Sometimes the school has to give your information to other people, such as the government, but it will only give away your information when you say it's ok or when the law says that they have to. When your data is given to someone else, they must look after it and keep it safe.

Why do we collect and use your information?

We will only collect your information when we need it to help us do our job or to follow the law. When we've collected it, here's how we use it:

- To support your learning.
- To monitor and report on your progress.
- To provide appropriate support and pastoral care.
- To assess the quality of what we do,
- To keep you safe (for example, food allergies information, emergency contact details, CCTV).
-
- To meet the statutory duty placed upon us to report infectious diseases e.g. supporting the Covid-19 test and trace system.
- To meet the statutory duties placed on us for the Department of Education (DfE) data collections.
- To record our own school history.

What information do we collect?

The categories of information that the school collects, holds and shares include the following:

Your personal information

This is things like your name and address.

Your characteristics

This means information about you, like where you're from, what language you speak and things like that.

Your attendance information

We will also record how many times you missed school and why you couldn't come to school We will also record details of previous schools you attended.

Your assessment information

We collect your test results when you sit a big test or exam.

Some of your medical information

We keep information about any times you've been ill and any special conditions you have that we need to know about to keep you safe. This includes information about allergies.

Your special educational needs

We collect information that helps us teach you better, such as any special educational needs you may have.

Behavioural information

We record if you have been excluded (hopefully never!) and why. We will also record if you have a behaviour management plan

Photography, Images and Recordings

Using photographs of you counts as processing your personal data. Before we take or use any photographs we will ask you (if you're old enough) or a parent to give permission for us to take and use pictures of you. We might use your pictures on display boards or on the school's website, for example. We may also record your image and voice recordings for assessment, celebration and in CCTV (to keep you safe).

Do you have to give us your information?

Yes - the information that we are required by law to process you must provide. If we ask you for information that you don't have to give us, we will ask for your permission and let you know why we want it and what we will do with it. If you don't want us to have the information that is your choice.

How long will we keep your information?

We don't keep it forever, only for as long as we need it to help us do the thing we needed it for. We have a policy that tells us when to keep it and when to bin it.

Will your information be shared?

We won't share your information with anyone else without your permission, unless the law says we can or should. For example, we routinely share information with:

- Schools or colleges that you attend after leaving us.
- Our Local Authority (Cumbria County Council).
- Child development and protection partners like our local Authority Children's Services, Public Health, Inclusion & Social Care etc. to check attendance, monitor, and protect children; private companies offering counselling and other family or support services.
- The Department for Education (DfE).
- The school nurse, medical services and NHS
- Third Party software providers.
- Government departments like Public Health England, Local Authority Public Health, and District Council Environmental Health Departments to comply with the law and support public health emergency action;
- Voluntary and charitable organisations (with your permission only), such as Barnardo's, our local Foodbank and similar organisations who can offer families practical help and support.
  For details of the information that we share with them please visit: https://www.gov.uk/education/data-collection-and-censuses-for-schools

Sometimes we have to share your information. We normally have to share it with the people in charge of all schools, the Department for Education (DfE). They may ask us to share things like:

- Pupils on roll at the school.
- Attendance figures.
- Performance data.

We share this information with the DfE under what is known as regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

They store some of their information in the National Pupil Database, and then share some of it with people looking to help schools and pupils like you. But don't worry, the database is very safe and your information won't get lost or given to anyone who shouldn't have it.

Once you reach the age of 13, we have to pass on certain information to the people in charge of local schools called the Local Authority. We might share some information with people who provide education and training for people over 16, like colleges. We may pass on information that helps them to make sure they provide the right kinds of education, such as your name, date of birth, where you're from and things like that. This information is always transferred securely.

Your parents can ask us to only share your name, address and date of birth, and nothing else, by sending an email or letter to Mrs Blamire, Office Manager at Kirkbie Kendal School. When you're 16, it's up to you to decide what information you want to share.

We have to share some information with careers services once you reach 16. We must provide both yours and your parents' names and address, and any further information relevant to the support services role; this will include telephone contact details. This enables the local authority to provide services as follows:

- Youth support services
- Careers advice and guidance If you require more information on how Connexions use your information please go to: https://careerconnect.org.uk/Privacy-Policy-i55.html

What are your rights?

You and your parents have the right to:

- Be told how we use your information.
- Ask to see the information we hold.
- Ask us to change information you think is wrong.
- Ask us to remove information when it's not needed anymore.
- Ask us to only use your information in certain ways.
- Tell us you don't want your information to be processed.

If the information we are collecting is information that you can choose not to give, you can tell us to stop collecting it at any time. If you're worried about how we get and use your information, you can speak to Mrs Eastwood at the school, who will be able to help you and answer any questions that you have. If you want to speak to somebody not at the school, you can call the people who look after information, called the Information Commissioner's Office (ICO), on 0303 123 1113 or using their live chat.

Four important things to understand

Now you've read this, we hope you understand that:

- The law requires us to get and use your information to help us do our job.
- We may share your information with others, but only when we really need to.
- We will ask for your permission to share your information whenever you have a choice.

You can tell us not to share your information, even when you have said yes before. If you have any questions, Mr Harris or Mrs Eastwood will be happy to help you.

Appendix C

SCHOOL PRIVACY NOTICE FOR STAFF
(How we use workforce information)

Kirkbie Kendal School is the data controller under the UK General Data Protection Regulation (UK GDPR) for the use of personal data explained in this Privacy Notice.

The categories of school workforce information that we process includes:

- Personal information like name, address, contact details, employee or teacher number, national insurance number & bank account details.
- Special categories of data like medical information for emergency or occupational health reasons; criminal conviction or social care action information for legal and safeguarding reasons; and protected characteristics information like gender, age, ethnic group etc.
- Contract information like start dates, hours worked, post, roles, salary information, and pre-employment vetting information like references;
- Work absence information like the number of absences and reasons;
- Qualifications and, where relevant, subjects or specialisms taught.

Why we collect and use this information

We use school workforce data to:

a) Provide us with a comprehensive picture of our workforce, how it is deployed, how it can be developed, and how it can be kept safe;

b) recruit appropriately and to inform the development of recruitment and retention policies;

c) enable individuals to be evaluated and developed in their career and be paid.

Under UK GDPR, the lawful bases we rely on for processing for processing personal workforce information are:

6(1)(b) to enter into or carry out a contract e.g., to employ people or buy and use services.

6(1)(c) to comply with the law e.g., recording sickness absence for benefits purposes, data sharing with child protection partners like social care, the NHS, and the Local Authority etc.

6(1)(a) having consent e.g., to use images and names in publicity.

When we process sensitive personal information like medical data or criminal history, we rely on lawful bases:

9(2)(a) having consent e.g., for referral to occupational health or other support services.

9(2)(b) to comply with the law e.g., pre-employment criminal record checks, providing reasonable adjustments for work or interview.

9(2)(h) for preventative or occupational medicine or to assess the work capacity of an employee;

9(2)(i) to improve public health e.g. we are required to report infections, like meningitis, Covid-19[1] or e-Coli, to local and national government departments;

9(2)(f) to make or defend legal claims e.g., some special educational needs records which include details about the staff involved, and all accident records etc.

This list is not exhaustive. For more information about the categories of information we process and why please see http://www.kirkbiekendal.cumbria.sch.uk/policies--procedures/152.html.

Collecting school workforce information

We collect personal information via recruitment application processes including references, employment contracts and payroll systems.

Most of the information we ask for is required by law or necessary so we can run the school effectively and some of it is voluntary. To comply with UK GDPR, if you have a choice about providing information, we will tell you when we ask for it.

Storing school workforce information

We hold school workforce data securely in line with the Information and Records Management Society (IRMS) Records Management Toolkit for Schools. Most data about staff is kept for between 6 months and 6 years after an event or the ending of a contract, although some is kept for much longer e.g., first aid and accident records that also involved children. Unsuccessful applicant data is kept for 6 months after the date of appointment. For more information about how long we keep some information for and why (data retention), and how we keep the data safe, please see our GDPR Policy and Data Protection Policy.

Who we share school workforce information with and why

We do not share information about our workforce with anyone without consent unless the law and our policies allow us to do so. The laws listed in this notice that require us to collect information also require us to share it. Data is transferred securely by hand delivery or registered post, via a government data transfer system like School to School, via a contractor's secure data sharing system like our online school trips safety system, and sometimes in other secure ways.

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring (see next section).

We also share school workforce information with:

- our payroll and pensions service provider to pay people;
- the Local Government Pension scheme (Your Pension Service) to manage pension contributions;
- HMRC for legal and tax reasons;
- organisations involved with our children like the local authority or other partner professionals who need the names, job titles, contact details and perhaps qualifications of our employees, the places we take children to on trips who might need more personal information like next of kin and medical needs, and workforce development organisations like training providers;
- Public Health England and, to support test and trace and similar public health emergency action, other partners like the NHS, Local Authority Public Health, and District Council Environmental Health Departments;
- Occupational Health and similar staff support services only with the consent of the individual.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. The law requires us to share information about our school workforce with the Department for Education (DfE) for the purpose of those data collections, under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under UK GDPR, you have the right to request access to information about you that we hold. To make a request for your personal information, contact our Data Protection Officer, Amanda Eastwood tel: 01539 727422 or email aeastwood@kksa.co.uk

Depending on which lawful basis above was used to process the data, you may also have a right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress,
- prevent processing for the purpose of direct marketing,
- object to decisions being taken by automated means,
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/.

For further information on how to request access to personal information held centrally by DfE, please see the 'How Government uses your data' section of this notice.

Withdrawal of consent and the right to lodge a complaint

If we are only processing your personal data because you consented, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting Data Protection Officer, Amanda Eastwood tel: 01539 727422 or email aeastwood@kksa.co.uk.

Last updated

This privacy notice was compiled using DfE advice and model documents. We may need to review it periodically, so we recommend that you revisit this information from time to time. This version was last updated on 14 October 2021.

Contact

If you would like to discuss anything in this privacy notice, please contact our Data Protection Officer, Amanda Eastwood tel: 01539 727422 or email aeastwood@kksa.co.uk

How Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Sharing by the Department

The Department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

How to find out what personal information DfE hold about you

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to

- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the DfE, you should make a 'subject access request'. Further information on how to do this can be found in the DfE's personal information charter published at: www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact the department: www.gov.uk/contact-dfe.

Appendix D

SCHOOL PRIVACY NOTICE FOR GOVERNORS
(How we use governance information)

Kirkbie Kendal School is the data controller under the UK General Data Protection Regulation (UK GDPR) for the use of personal data explained in this Privacy Notice.

The categories of school workforce information that we process includes:

- personal information like name, date of birth, gender identity, contact details including address and postcode;
- financial or business information like a governor's outside financial or business interests, or bank details for expense payments;
- Special categories of data like criminal conviction or social care action information for legal and safeguarding reasons, next of kin and medical information (to prevent or manage a health or medical issue), and protected characteristics information like gender identity or religion.
- governance details like their role, start and end dates and governor ID.

Why we collect and use this information

The personal data we collect is essential to fulfil our official functions and meet legal requirements.

We are an academy and have a legal duty under the Academy Trust Handbook to provide governance information to the Get Information About Schools (GIAS) scheme online.

We also use governor data to:

a) comply with the law and keep governors safe;
b) recruit appropriately; and
c) enable individuals to be paid expenses.

Under UK GDPR, the lawful bases we rely on for processing personal governance information are:

6(1)(b) to enter into or carry out a contract e.g., to appoint governors, include them in services we buy like access to online subscriptions we hold, or to engage with our training or activity providers.

6(1)(c) to comply with the law e.g., publishing information on our website and submitting data to GIAS.

6(1)(a) having consent e.g., to use images and names in publicity.

When we process sensitive personal information like medical data or criminal history we rely on lawful bases:

9(2)(a) having consent e.g., for referral to occupational health or other support services.

9(2)(b) to comply with the law e.g., pre-appointment criminal record checks, providing reasonable adjustments to governor tasks or election procedures.

9(2)(i) to improve public health e.g., we are required to report infections, like meningitis, Covid-19[1] or e-Coli, to local and national government departments;

9(2)(f) to make or defend a legal claim e.g., all accident records etc.

This list is not exhaustive. For more information about the categories of information we process please see our Publication Scheme.

Collecting governance information

We collect personal information via governor application forms. Most of the information we ask for is required by law or necessary so we can run the school effectively and some of it is voluntary. To comply with data protection legislation, if you have a choice about providing information, we will tell you when we ask for it.

Storing governance information

[1] Visit: https://www.gov.uk/guidance/maintaining-records-of-staff-customers-and-visitors-to-support-nhs-test-and-trace#information-to-collect, if you want more information about Test and Trace, what data they collect and what they do with it.

We hold governor data securely in line with the Information and Records Management Society (IRMS) Records Management Toolkit for Schools. Most data about governors is kept for between 6 months and 6 years after an election or term of office ends, although some is kept for much longer e.g., minutes of governor meetings showing attendees are kept for the lifetime of a school. For more information about how long we keep some information for and why (data retention), and how we keep the data safe, please see our Data Protection Policy and data asset register.

Who we share governance information with and why

We do not share information about individuals in governance roles with anyone without consent unless the law and our policies allow us to do so. The laws listed in this notice that require us to collect information also require us to share it. Data is transferred securely by hand delivery or registered post, via a government data transfer system like GIAS, and sometimes in other secure ways.

We routinely share governor information with:

- our local authority (as above),
- our financial services provider to pay expenses;
- Public Health England and, to support test and trace and similar public health emergency action, other partners like the NHS, Local Authority Public Health, and District Council Environmental Health Departments
- other organisations like an off-site training or activity provider that needs next of kin or medical details to manage them safely, and third-party service providers like online subscriptions, but usually only with consent.

Sharing with the Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections.

We are required to share information about individuals in governance roles with the (DfE) under the requirements set out in the Academy Trust Handbook . All data is entered manually on the GIAS system and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under UK GDPR, you have the right to request access to information about you that we hold. To make a request for your personal information, contact Data Protection Officer, Amanda Eastwood tel: 01539 727422 or email aeastwood@kksa.co.uk:

- Depending on which lawful basis above was used to process the data, you may also have a right to:
- object to processing of personal data that is likely to cause, or is causing, damage or distress,
- prevent processing for the purpose of direct marketing,
- object to decisions being taken by automated means,
- in some circumstances, have inaccurate personal data rectified, blocked, erased, or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/.

For more information on how to request access to personal information held centrally by the DfE, please see the 'How Government uses your data' section of this notice.

Withdrawal of consent and the right to lodge a complaint

If we are only processing your personal data because you consented, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting Data Protection Officer, Amanda Eastwood tel: 01539 727422 or email aeastwood@kksa.co.uk.

Last updated

This privacy notice was compiled using DfE advice and model documents. We may need to review it periodically, so we recommend that you revisit this information from time to time. This version was last updated on 29 October 2021.

Contact

If you would like to discuss anything in this privacy notice, please contact: Data Protection Officer, Amanda Eastwood tel: 01539 727422 or email aeastwood@kksa.co.uk.

How Government uses your data

The governance data that we lawfully share with the DfE via GIAS will:

- increase the transparency of governance arrangements;
- enable maintained schools and academy trusts and the department to identify more quickly and accurately individuals who are involved in governance and who govern in more than one context;
- allow the DfE to be able to uniquely identify an individual and in a small number of cases conduct checks to confirm their suitability for this important and influential role.

Data collection requirements

To find out more about the requirements placed on us by the DfE including the data that we share with them, go to https://www.gov.uk/government/news/national-database-of-governors

Note: Some of these personal data items are not publicly available and are encrypted within the GIAS system. Access is restricted to a small number of DfE staff who need to see it in order to fulfil their official duties. The information is for internal purposes only and not shared beyond the department, unless the law allows it.

How to find out what personal information DfE hold about you

Under the terms of the UK Data Protection Act 2018, you're entitled to ask the Department:

- if they are processing your personal data;
- for a description of the data they hold about you;
- the reasons they're holding it and any recipient it may be disclosed to;
- for a copy of your personal data and any details of its source.

If you want to see the personal data held about you by the DfE, you should make a 'subject access request'. Further information on how to do this can be found in the DfE's personal information charter published at: www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact the department: www.gov.uk/contact-dfe.

Appendix E

Kirkbie Kendal School

Parental Consent Form - Trips, Images and Pain Relief

Name of Child: ..... **Date of Birth:** ..... **Class/Group:** .....

EDUCATIONAL VISITS

This consent will last for the entire time your child is with us at Kirkbie Kendal School, but it is good practice for us to check your consent still applies when we offer residential or adventurous visits. When we tell you about them, we will ask for current information about your child e.g. updated medical needs, sleepwalking, swimming ability etc. and offer you the chance to withdraw your consent. You should also complete and return any slip provided then.

Declaration *Please delete as applicable

I ***do / do not*** consent to my child taking part in Kirkbie Kendal School trips and other activities that take place off-site **and** to them being given urgent medical or dental treatment or necessary pain relief during any trip or activity.

I understand that:

- **All** trips and activities are covered by this consent and will include;
  - all visits (including residential trips) which take place during the holidays or a weekend,
  - adventure activities at any time *and*
  - off-site sporting fixtures outside the normal Kirkbie Kendal School day,
- Kirkbie Kendal School will provide me with information about each trip or activity before it takes place.
- I can inform Kirkbie Kendal School that I **do not** want my child to take part in a particular trip/activity and I should do so in writing.
- I **must** ensure that I and my child understand and agree to abide by any trip Code-of-Conduct.
- I **must** keep Kirkbie Kendal School informed if any medical information I have provided becomes out-of-date or where religious beliefs may impact on any medical treatment my child may receive.
- I **must** keep Kirkbie Kendal School informed if any emergency contact information I have provided becomes out-of-date or does not apply to a particular trip and I must provide alternatives as necessary.
- All Kirkbie Kendal School activities are appropriately insured. I also understand the extent and limitations of this insurance (details available on request).

Medical Information: Details of any medical conditions including allergies and travel sickness that my child suffers from and any medicines with dosage etc. that they should take during off-site activities including those outside Kirkbie Kendal School hours or overnight – attach additional sheet if necessary.

Using our website or an app to stay in touch: *please delete as applicable

To keep up to date with information about Kirkbie Kendal School, particularly activities, visits and fixtures:

I ***can / cannot*** use the Kirkbie Kendal School website.

I ***can / cannot*** use the Kirkbie Kendal School apps (Edulink and Parentmail).

EMERGENCIES:	**Emergency Contact 1**	**Emergency Contact 2**
Name:		
Relationship:		
Telephone Number(s): Work:		Work:
Home:		Home:
Mobile:		Mobile:

Appendix F

Kirkbie Kendal School

Parental Consent for Image and Voice - Conditions of Use

- This form is valid for the period of time your child attends the School. The consent will automatically expire after this time. We will not re-use any photographs or recordings after your child leaves the school without additional consent.
- We will not generally use the personal details or full names (which means first name and surname) of any child or adult in a photographic image, on video/DVD, on our website, in our prospectus or in any of our other printed publications, unless there is a reason for doing so (e.g. if a child has won a prize or to celebrate student success).
- We will not include personal addresses, emails, telephone numbers, fax numbers on video, on our website, in our prospectus or in other printed publications.
- If we use photographs of individual children, we will usually not use the name of that child in the accompanying written text or photo caption unless there is a reason for doing so (e.g. if a child has won a prize or to celebrate student success).
- We may include pictures of children and staff that have been drawn by the children.
- We do use group photographs or footage with general labels, such as 'making Christmas decorations.'
- We will only use images of children who are appropriately dressed.
- We may discuss the use of images with children in an age appropriate way to role model positive behaviour.
- This consent can be withdrawn by parent/carer at any time by informing the School in writing.

		Please Circle as Appropriate
1	May we use your child's photograph/image in displays around the school?	Yes / No
2	Do you consent to your child being included in any image or voice recordings made by other parents/carers who want to make a recording of school events for their own person use, e.g. school concert, drama production? **If consent is given, please also sign the attached letter.**	Yes / No
3	May we use your child's photograph/image in our prospectus and other printed publications that we produce for educational and promotional purposes?	Yes / No
4	May we use your child's image on our website or other electronic communications (e.g. the school's official Twitter page/electronic newsletter)?	Yes / No
5	Are you happy for your child to appear in the media e.g. if a newspaper photographer or television film crew attend an event organised by the school?	Yes / No
6	Do you give consent for your child's name to be published in the media?	Yes / No

I have read and understood the conditions of use and I am also aware of the following:

- Websites can be viewed throughout the world and not just in the United Kingdom where UK law applies.
- I/we will discuss the use of images with our child/ren to obtain their views, if appropriate
- As the child's parents/guardians, we/I agree that if we/I take photographs or video recordings of our child/ren which include other children then we will only use these for personal use.

Name of Child: _____ Date: _____

Parent/Carer Name: _____

Parent/carer's signature: _____

Appendix G

Kirkbie Kendal School

CCTV PROCEDURES

Contents

CCTV PROCEDURES

1. Definitions, References and Useful Links

Data controller:	Usually an organisation rather than a person that determines the purpose and means of processing personal data.
Data processing:	Anything that is done with data e.g. recording, displaying, using, changing, storing, transferring, deleting etc.
'Data Protection by Design':	The integration of appropriate technical and organisational measures to protect personal data and an individual's right to privacy from the design stage throughout the whole life cycle of the data.
Data subject:	Anyone who is the subject of data we hold i.e. any person whose image we record using our CCTV.
Personal data:	Any data that can be used to directly or indirectly identify a living person i.e. their image.
Operator:	A member of staff who has received specific training in operating CCTV systems.

In developing our CCTV Procedures we have used the following guidance and with due regard for the following pieces of legislation which affect what we do:

- The Information Commissioner's Office (ICO) website: https://ico.org.uk/ more specifically:
  - the guidance: 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data', June 17;
  - the more detailed guidance: 'Data Protection Impact Assessments (DPIAs)', and
  - the 'Subject Access Code of Practice', June 17
- The Regulation of Investigatory Powers Act (RIPA, 2000)
- The Protection of Freedoms Act (POFA, 2012)
- The Data Protection Act (DPA, 2018)
- The Human Rights Act (HRA, 1998)
- The Equality Act (EA, 2010)
- The Home Office guidance: Surveillance Camera Code of Practice, June 2013
- Our Data Protection Policy

2. Introduction

Kirkbie Kendal School (hereinafter referred to as 'the school') has in place a Closed Circuit Television (CCTV) system, both inside and outside of the buildings. It is a secure system of video cameras which transmits a signal to a specific place for display on limited monitoring devices and which can be recorded.

We recognise that our system collects personal data that is regulated by the European Union's (EU) General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA) 2018. These procedures detail the purpose, use and management of the system and how we will ensure that we comply with relevant legislation and safeguard the individual rights of our data subjects.

Our school is registered with the ICO as a Data Controller, our registration is updated annually and it includes our CCTV system. ICO Registration Number: Z3051354.

The individual named as responsible for the operation of the system is David Finch Anyone who wants to discuss our use of CCTV and the guidelines we follow can contact them on 01539 727422 and/or dfinch@kksa.co.uk during normal working hours.

We also have a Data Protection Officer whose contact details we publish on our website www.kirkbiekendal.cumbria.sch.uk so that anyone can easily raise any concerns they might have about our use of personal data, including our CCTV system.

In operating our CCTV we will follow the Information Commissioner's Office (ICO) guidance, *'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data', June 17*. It may also be necessary to refer to our Data Protection Policy e.g. for further guidance on protecting data transfers of CCTV images.

These Procedures will be subject to regular review. If a new or additional system is being considered, the review will involve a 'Data Protection by Design' approach using a Data Protection Impact Assessment (DPIA) including consultation with the affected school community e.g. staff, students, parents etc. where appropriate.

Our aim is to ensure we avoid recording and storing excessive amounts of personal data.

3. Description & Objectives of the CCTV Scheme

The CCTV system comprises of 22 fixed and moving cameras without audio recordings located around the site both internally and externally which function 24 hours a day throughout the year for the purposes of:

- protecting the buildings, assets and personal property on site;
- enhancing the personal safety of staff, students and members of the public such as visitors;
- reducing the fear and potential incidence of crime including theft and vandalism;
- reducing the fear and potential incidence of anti-social and harmful behaviours like bullying or hate crimes;
- supporting the Police in order to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders; and
- ensuring that site rules are respected so that the school can be properly managed.

3.1 System and Equipment

When we decided what system to install, we chose one that can produce clear images which are useful for our purposes e.g. a large enough viewing area, high enough resolution and sufficient frames per second of movement to be able to identify undesirable behaviour and the perpetrators. We also made sure we have the technology to compress and share the data with the proper authorities such as the Police without negatively affecting the quality of recordings and therefore its usefulness.

We regularly review our use of CCTV and we can change the way it operates if necessary to better protect people's privacy. For example: we can make it so that certain cameras record only at certain times of day when we have identified that the problem we need to monitor occurs and not at times when we know it doesn't.

3.2 Camera Siting

When deciding where to put cameras, we tried to put them in plain sight and in places where they can capture clear images of the spaces we need to monitor, while avoiding the capture of any images (or any clear images) of people who are not using or visiting our premises e.g. passers-by or the gardens, driveways etc. of our neighbours.

CCTV monitoring of public areas may include:

Protection of buildings, assets, property and personal property: at building perimeters, entrances & exits, lobbies & corridors, special storage areas, cashier locations, receiving areas for goods/services.

- **Video patrol of public areas:** on parking areas, main entrance/exit gates, traffic control areas.
- **Providing evidence for internal disciplinary action or external criminal investigation (carried out by the Police):** surveillance of misconduct, bullying and other undesirable behaviours; robbery, burglary and theft surveillance.

No moving camera is sited in any area where it can capture clear images of unintended or overlooked spaces when an operator moves it. Cameras are also never sited anywhere that people have a reasonable expectation of privacy e.g. toilets and changing rooms.

We also considered how the location environment might affect recording quality e.g. too much or too little daylight; insufficient night-time illumination; plant growth or summer foliage obscuring the lens; vulnerability to vandalism etc.

3.3 Notification and Signage

These CCTV procedures describe the purpose and location of CCTV monitoring and include the contact details for the system manager in the Introduction so that anyone who wants to discuss our use of CCTV and the guidelines we follow can contact them.

These procedures are freely available to all staff on the secure staff-only information network. A copy can be provided on request to staff, students, parents, carers or other visitors.

Our community and the general public are made aware of the presence of CCTV by appropriate signage at the entrance to a surveillance zone and this is reinforced with further signage inside some areas. Our signs:

- are clearly visible and readable e.g. large enough to be noticed, larger print if meant to be seen from a vehicle, more prominent and/or frequent in places where people might not expect to find CCTV, or where the system is so discreet people can't easily see that they are being monitored;
- include details of the organisation that operates the system, why surveillance is being used and who to contact about the scheme (where these things are not obvious to those being monitored e.g. if we use a security company to operate our system for us);
- include basic contact details for the system manager, either a website address where contact details can be obtained or a telephone number.

A typical example warning sign for use on our premises can be found at Appendix C.

4. Management Roles and Responsibilities

4.1 The Head teacher or Manager

The Head teacher is responsible for day-to-day operations including an overview of all data protection matters. With regard to CCTV specifically, they are responsible for:

- ensuring the system in use is broadly fit for purpose and has a suitable maintenance scheme in place;
- ensuring the system is properly registered with the ICO, that people affected by the CCTV are informed about it, and that processing of the data is fair, lawful and not excessive;
- ensuring mechanisms exist to provide all staff and other relevant individuals, such as agency workers, with suitable information and/or training to enable them to follow these procedures;
- promoting the development of good data management practice, leading by example and encouraging good information handling practice;
- authorising the release of CCTV data to any third parties;
- approving any temporary extension of the CCTV system to cover special events that have particular security or access & communication requirements, and ensuring proper withdrawal afterwards. (This is not the same as approval for mobile equipment or covert surveillance being used for very serious or criminal investigations – please see Section 5.3: Covert Surveillance).

Any of these tasks can and may be delegated to other suitably competent managerial staff, but they remain a management responsibility of the headteacher or manager.

4.2 The System Manager

The CCTV system manager is responsible for the day-to-day running of the system to include:

- Periodic checks of the hardware and the siting of it e.g. plant growth, vandalism etc.;
- Ensuring software, especially security updates are successfully applied as necessary;

- Carrying out the periodic tasks required e.g. monitoring data, checking storage arrangements are still suitable, ensuring data has been properly deleted etc.;
- Keeping comprehensive and accurate records of all data, surveillance and CCTV footage, and the processing of it, especially the storage of any recorded data and its deletion;
- Collecting and presenting useful data to the SLT regarding the effectiveness of the system.

This person will also be available during normal operating hours and will understand and have available to them all relevant policies, procedures, technical and security information about the CCTV system to enable them to answer queries or help solve problems.

4.3 The Data Protection Officer (DPO)

There is no specific role for our DPO in managing our CCTV systems. They have more general data protection responsibilities such as:

- conducting or advising on our Data Protection Impact Assessment if we want to extend our surveillance or significantly change something about how we operate it;
- raising awareness of data protection issues which might include the proper use of CCTV;
- monitoring our own monitoring (records) of our CCTV practice;
- reporting on data protection compliance to the governing body which could include the effectiveness of our surveillance; and
- reporting data protection breaches to the ICO.

Our DPO is therfore required to liaise with CCTV operators and the system manager to adequately support them with the data protections aspects of their work.

4.4 CCTV Operators who are our CCTV operators?

All CCTV operators are members of staff suitably authorised to carry out their role and who have received specific training in:

- arrangements for recording, retaining and deleting CCTV data in line with data protection laws;
- handling information securely;
- responding appropriately to requests for information e.g. from staff, individuals, the police etc.; and
- recognising a Subject Access Request and how to respond.

Operational expectations of CCTV operators are set out in Section 5: System Operation.

The two key ways we have tried to assure that we can meet our legal obligations in the protection of personal data are having appropriate access controls to data storage, and having robust encryption. Staff of the security company have been made aware of their obligations relating to the security of data.

Our service contracts are usually deemed commercially sensitive documents and are not made generally available. Staff who need to see any contract detail with any supplier in relation to their work can make an appropriate request to David Finch, IT Manager.

5. System Operation

During normal operating hours, the CCTV surveillance scheme will be administered and managed by the the System Manager in accordance with the principles and objectives expressed in these procedures, although day-to-day tasks and some key monitoring tasks will be delegated to suitable and trained individuals.

Outside normal operating hours, the Site Manager will administer the scheme where issues arise. Our DPO or a suitable member of the SLT will also be available remotely for advice.

CCTV will generally operate 24 hours a day on every day of the year and the following conditions will apply to all live feeds and data recordings.

5.1 Live Visual Feeds and Data Recording

All cameras are monitored in reception and in the site managers office. The site manager, network manager and the helpdesk have access to all cameras and their recordings, the data is only available to selected trained and authorised staff.

Our CCTV system will not be used to monitor normal teacher/student classroom activity.

CCTV monitoring based on individual characteristics protected under the EA 2010 and other related legislation (race, gender, pregnancy, sexual orientation, national origin, disability etc.) is strictly prohibited. The system is in place to monitor suspicious activities and not individual characteristics.

Monitoring for the purposes of security and personal safety will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies and personnel for other purposes is prohibited e.g. the monitoring of political or religious activities, or monitoring employee and/or student evaluations for reasons that are not compatible with those clear security and safety objectives.

Unless an immediate response to events is required, operators will not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained for Directed Surveillance to take place, as set out in the RIPA 2000 (see Section 5.3).

When a camera zoom facility is being used, a second person will be present with the camera operator to best ensure that there is no unwarranted invasion of privacy.

Materials or knowledge secured as a result of CCTV monitoring will only be used for the purposes of ensuring security and personal safety. Data will only be published in the course of the legitimate investigation of a specific crime and this will normally be on the advice of law enforcement or another relevant public authority. Data will never be released in any medium for the purposes of entertainment.

Information obtained through the CCTV system may only be released when authorised by the Head teacher/Manager following consultation with the Chair of the Governing Body. Any requests for CCTV recordings/images from the Police will be fully recorded. If a law enforcement authority is seeking a recording for a specific investigation, any such request made should be made in writing.

5.2 Live Audio Feeds and Data Recording

Recording conversations between people, especially members of the public, is highly intrusive data monitoring and not something easily justified. Our CCTV system is capable of audio recording but our cameras are either not capable or not physically configured to do so.

5.3 Covert Surveillance

The UK Home Office *'Covert Surveillance and Property Interference Code of Practice' (Dec 2014)* says that, "surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place" (section 1.10, p7).

Directed surveillance at particular individuals in a covert manner is not something we will engage in except in exceptional circumstances where serious or serial criminal offences are being committed which carry a maximum penalty of at least 6 months imprisonment. We must act in accordance with the RIPA 2000. It is much more likely that we will cooperate fully with any covert surveillance the police or other appropriate public authority receives the proper court authorisation to carry out involving our premises or organisation e.g. if serious fraud was being perpetrated against us.

We will seek appropriate advice before becoming involved in any RIPA related actions.

5.4 Control Room Operations (For live feeds, Reception and site manager. For data storage, server room)

The viewing of live CCTV feeds is restricted to:

specific trained staff in a 'staff only' access area when the display includes footage of areas which are **not** in plain sight of people who can see the feed display monitor.**Server room control room operations will include:**

- A daily check on the efficiency of the system, in particular that equipment, including software updates and the means to raise the alarm in an emergency or other relevant incident, is working properly.
- Ensuring cameras are not directed at individuals, their property or a specific group of individuals unless in direct response to unfolding events to better achieve system aims e.g. enhanced safety and security by identifying issues and the people involved.
- Administrative functions like maintaining secure data streams and adequate recording space, filing and maintaining incident and system maintenance logs.

Live viewing control room operations will include:

- Following strict protocols when allowing normally unauthorised persons e.g. untrained staff, contractors or visitors, entry to the control room as follows:
  - Being satisfied about the control room visitor's identity and legitimate reasons for entry e.g. an untrained member of staff receiving training; a contractor carrying out servicing and maintenance work; a visitor who has been granted permission to view specific images of themselves; a parent who is being shown evidence of an incident involving their child; a police officer involved in a criminal investigation using the data; another representative with legitimate reason e.g. from the Department for Education, the Health & Safety Executive etc.
  - Refusing access to unauthorised persons when their identity or legitimate reasons are in doubt.
  - Adequately supervising control room visitors throughout their visit.
  - Keeping a record of all control room visitors in the log book including visits by normally unauthorised staff (visitor name, date & time of entry and exit, reason for entry, name of operator who supervised them).
  - Adequately protecting people's data protection rights when visitors are in the control room e.g. turning live feed monitors away or off (after ensuring data not being monitored live is being recorded instead), curtailing the visit if circumstances demand it.

The control room will always have at least one trained operator in it or it will be locked.

Recordings will only be made by authorised staff who will only make them available for viewing by authorised staff, authorised visitors, or an appropriate public authority, in the control room or in another suitable and restricted area, such as a secure office.

6. CCTV Data Handling

6.1 Storage

CCTV data storage facilities have been designed to ensure the integrity of the data being stored is maintained so it can be used effectively for its intended purpose i.e. storage arrangements do not significantly degrade the data making it less useful.

We adequately protect this data using a mixture of operational security measures such as restricting access to trained/authorised users and locking areas where it is stored or can be viewed, and technical security measures such as encryption, secure networks and personal logins that are never shared. We also keep records of routine access through the system's own performance monitoring logs, and records of non-routine systems access via the log book.

CCTV operators receive training in data protection relevant to their specific role and all staff can find information about their responsibilities in our Data Protection Policy. All staff and relevant others such as contractors are made aware and reminded regularly that misuse of our CCTV may result in disciplinary and/or criminal proceedings against them.

Any storage of CCTV data on any kind of removable media e.g. tapes, DVDs, USB devices etc. is strictly controlled with checks in place to ensure that it:

- can only be done by a trained operative;
- does not interrupt normal CCTV operations;
- does not degrade the data or remove important date and time stamping;
- provides the information in a suitable format which is straightforward to use;
- is recorded in the automatic or manual log book, including the final destination where ownership of the record or a copy of the record has passed to a third party e.g. police, the person in the images etc.
- is appropriately and securely stored, including sealed against tampering if being kept as evidence in any kind of proceedings.

When recording or transferring CCTV data to removable media:

- Each device will be marked with a unique reference point to easily identify it from any other.
- Each device will be suitably wiped clean of any previous data *before* subsequent recordings are transferred to it.
- Devices or data files on a device will be appropriately marked with start and end times and dates and any other important information such as camera reference/location etc.
- Devices required for evidential purposes will be appropriately sealed against tampering in front of a suitable witness, signed off by the system manager or head teacher on behalf of our organisation as the data controller, and stored securely but separately from other recordings in readiness for handover to the proper authorities.
- When CCTV data has been sealed, it can be unsealed provided there is good reason e.g. a copy needs to be made for handover to the police – this unsealing must be done in front of an appropriate witness who is present until the original data is resealed and an appropriate record has been made in the log book which includes details of the witness.
- Any copies made for evidential purposes will be handed over to the proper authorities at the earliest opportunity and a copy retained until the conclusion of any legal action.

6.2 Retention

Legislation requires that personal data is only kept for as long as is necessary to achieve the outcomes that it was processed for in the first place. It does not dictate how long we can retain data such as CCTV recordings and we only need to have a clear and justifiable policy decision to keep it.

Our retention schedule has some flexibility in it and is determined by:

- the purpose for which the information is being collected and how long it is needed to achieve this purpose;
- the settings we have selected for routine and automatic deletion, currently 21 days on the basis of how long it has taken in the past to discover, properly investigate and deal with issues;
- our procedure for temporarily extending the retention period in a routine way, for example, over the entire summer holiday period to ensure surveillance remains effective at a potentially risky time of year for the premises;
- what appropriate public authorities such as the police require us to retain and for how long in the interests of a criminal prosecution.

When we review this retention schedule we will look at our current practice and ask:

- Have we decided on the shortest possible retention period based on our reasons for keeping data?
- Do all relevant staff, especially the CCTV operators or system manager, understand our retention schedule?
- Are measures are in place to ensure the permanent deletion of information through secure methods at the end of this period?
- Are the checks we carry out systematic and do they include compliance with the retention period in practice?

Retention is a key question in the annual system review at **Appendix A**.

6.3 Access & Disclosure

CCTV data is secured against unauthorised access using a range of organisational and technical security measures and good record keeping as described in Sections 5 and 6 above.

Unless a live CCTV feed is displayed publicly and allows viewers to see only what they can see by looking around them, only trained operators and specially authorised people are permitted to view live CCTV feeds or recordings. This data can only be viewed for a reason compatible with why the system was installed in the first place, or in accordance with an individual's rights under the DPA 2018. For more information about what people's rights to data protection are and how we uphold those rights please read our Data Protection Policy.

Requests to access CCTV data from people not normally authorised to view it, including staff, must be made in writing and the decision and subsequent action recorded. Examples may include:

Example 1: to detect and prevent crime

In reporting a burglary, the headteacher provides information to the police about images of the perpetrators captured in CCTV footage.

The headteacher can invite police to the Control Room and authorised them to view the data. If they deem the data useful to their criminal investigation, a copy can be provided and the appropriate authorisation and disclosure record must be completed. If the police also request that the original data not be deleted until the conclusion of any legal proceedings, their direction on protecting the chain of evidence should be followed while they are present e.g. sealing the original media it is recorded on against tampering or adequately quarantining the original data stream from automatic system deletion and securing it against tampering with an additional security layer e.g. a file password.

Example 2: to maintain public safety

A parent asks to see the evidence on which school based disciplinary action against their child.

The headteacher can invite parents to a secure office area and authorise them to view footage of the incident which prompted the action, but it would not be appropriate to provide a copy. The footage may need to be an edited copy rather than the original to protect the privacy of individuals captured who are not already identified as being involved in the incident. The appropriate authorisation and disclosure record must be completed even where no copy of the data is provided.

Example 3: to uphold an individual's personal data rights (and potentially detect and prevent crime)

A visitor requests CCTV footage of the car park, which shows their car being damaged. They say they need it so that they, or their insurance company, can take legal action. This kind of request made by an individual is most likely to be a SAR and should be handled under those procedures outlined in our Data Protection Policy.

The headteacher should not authorise access or disclosure unless they are reasonably sure that the request is genuine and have assessed whether there is any risk to the safety of other people involved. The appropriate authorisation and disclosure record must be completed, even where a request is refused because the law requires us to justify our decisions and explain them to requestors.

Example 4: to maintain public safety (through having well trained staff)

The Assistant Headteacher with key leadership responsibility for behaviour management requests the CCTV footage of a potentially violent incident being expertly diffused by a teaching assistant to use in a whole staff meeting focussed on the development of positive behaviour management strategies.

The system manager should have received enough training to enable them to decide to agree to the request while imposing strict conditions on the use and storage of the copy made. The appropriate authorisation and disclosure record must be completed.

Example 5: to detect and prevent crime (and uphold our legal right to restitution)

Our insurance company requests CCTV footage in order to pursue a civil claim for compensation against the perpetrators of damage to school property.

The head teacher can authorise the making and secure transfer of a copy of the footage to a representative of the insurer, taking care to ensure that the identity of any person captured in the

footage who was not involved in the damage is properly protected. The appropriate authorisation and disclosure record must be completed.

The decision to authorise a person to view or receive a copy of CCTV data must be made at the appropriate level. When a normally unauthorised member of staff makes a request, the system manager is expected to use their training to make and properly record an appropriate decision on allowing the access. When the requestor is not a member of staff, the headteacher must agree and sign off on the request either granting access or denying it and giving the reasons.

With the exception of any court mandated order, we have the right to reasonably refuse any request for information that we feel does not comply with the DPA 2018 and we will give our reasons.

If the data recipient is a relevant public authority e.g. the police or court, it is always the recipient's responsibility to have regard for the ICO CCTV Code of Practice and to comply with any other legal obligations such as DPA 2018, HRA 1998 etc. in relation to any further disclosures.

CCTV data will never be released onto the internet.

Information may be released to the media for identification purposes which could include release to the internet, but this will only be done by a proper law enforcement agency or under their express and written direction.

Once we have disclosed information to another body or public authority, such as the police, insurance company etc. they become the Data Controller for the copy they hold. It is their responsibility to comply with the DPA 2018 and any other relevant legislation in relation to any further disclosures.

6.4 Subject Access Requests (SAR)

Our surveillance system and the management of it has been designed to take into account that we may need to comply with a SAR e.g. how easily data can be located, retrieved, transferred etc. CCTV operators have been trained to recognise and respond appropriately to a SAR.

Where a SAR is made involving CCTV footage it is now much less likely that images which include other people can be provided to individuals due to the difficulties there might be in adequately anonymising those other people. The update to legislation as a result of the GDPR draws a distinction between being able to identify someone directly from the data provided, but also being able to identify someone indirectly from the data provided together with other knowledge that people who see that data might reasonably already have or come by. Pixelating the features of an individual will not necessarily obscure their identity from people who know them very well, blurring an image may not sufficiently disguise a distinctive piece of clothing worn by a known associate etc. We understand how important it is that in upholding an individual's data protection rights, we don't breach the rights of anyone else.

Details of our full procedures for handling SARs can be found in our Data Protection Policy.

6.5 Freedom of Information (FOI) Requests

The Freedom of Information Act (FOIA) 2000 applies to us and we have a member of staff who understands our responsibilities and is responsible for responding to FOI requests within the 20 working days allowed from receipt of the request.

Section 40 of the FOIA contains a two-part exemption relating to information about individuals. If we receive a request for surveillance system information, we will consider:

- Whether the information is the personal data of the person requesting it. If so, that information is exempt from the FOIA. Instead this request should be treated as a data protection Subject Access Request (please see Section 6.4 above and our Data Protection Policy for more information about handling SARs).
- Whether the information is the personal data of other people. If it is, the information can only be disclosed if to do so would not then be a breach of the DPA 2018.

Personal data that is not solely about the requester or is not already intentionally and lawfully published in the public domain cannot be disclosed in response to a FOI request.

Personal data which is only about the person making the FOI request can be disclosed to them but never as a response to an FOI request. We will inform the enquirer that we cannot process their FOI request because the data they have asked for is personal and disclosure is not permitted under the FOIA, but that as the images are only of them, the information could be provided under the DPA 2018 provisions for individuals to make a SAR of any organisation which they think holds data about them.

7. Breaches

A breach of these procedures by staff, and in some cases students or others, *may* result in disciplinary action and will be thoroughly investigated by the most suitable and senior leader and/or independent investigator so that appropriate remedial and disciplinary action can be taken. Information obtained in violation of these procedures may not be used in disciplinary proceedings against an employee, or a student.

A breach of these procedures may also be a breach of our legal obligations under the GDPR and DPA 2018 and could be reportable to the ICO where a maximum fine of €20 million could be levied. Please refer to the relevant sections of our Data Protection Policy to find out how we handle breaches of this legislation.

8. Monitoring and Review

Routine performance monitoring, including random operating checks, may be carried out by the Head teacher/Business Manager.

These procedures will also be regularly reviewed, either by us internally or externally by a third party to ensure the standards established when the system was set up, are being maintained.

Appendix A will be used to carry out and record a periodic review, at least annually, of the system's effectiveness. This is so that we can ensure it is still doing what it was intended to do while adequately protecting people's rights and personal data. We will take into account the recorded results of the last review and:

- Why we need to continue using the system and how we justify data retention.
- How effective technical and organisational security measures have been at protecting the data.
- Whether information about operation of the system and how individuals can make access requests remains appropriate and available.
- Whether our commitment to the ICO Code of Practice remains clear and we provide suitable information about complaining to us, complaining to our DPO, or complaining to the ICO about our data protection compliance.
- Whether our monitoring of our own compliance is sufficiently regular and provides us with useful information that helps us understand how our system is being used and how we can best protect people who are affected by its use.

If a review determines that the system's effectiveness has diminished or it no longer achhieves its purpose, data processing will be stopped or appropriately modified as soon as is practicable.

9. Complaints

Any complaints about our CCTV system or the management of it should be addressed to the Head teacher, although anyone can also independently contact our DPO because we publish their contact details on our website.

Complaints will be investigated in accordance with our Data Protection Policy, our Complaints Procedure and these CCTV Procedures.

Appendix H

PROTECTION OF BIOMETRIC INFORMATION POLICY

1. KIRKBIE KENDAL SCHOOL ACADEMY TRUST PROTECTION OF BIOMETRICS POLICY STATEMENT

Kirkbie Kendal School Academy Trust is committed to protecting the personal data of all its students and staff, this includes any biometric data we collect and process.

We collect and process biometric data in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected. This policy outlines the procedures the school follows when collecting and processing biometric data.

2. BIOMETRIC INFORMATION AND HOW IT SHOULD BE USED

LEGAL FRAMEWORK

- This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Protection of Freedoms Act 2012.
- Data Protection Act 2018.
- General Data Protection Regulation (GDPR).
- DfE (2018) 'Protection of Biometric Information of Children in Schools and Colleges'.

- This policy operates in conjunction with the following School policies:

- Data Protection Policy.
- Records Management Policy.

3. DEFINITIONS

- **Biometric data**: Personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns, and hand measurements.

- **Automated biometric recognition system**: A system which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.

- **Processing biometric data**: Processing biometric data includes obtaining, recording or holding the data or carrying out any operation on the data including disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

  - Recording student/staff biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.
  - Storing student/staff biometric information on a database.
  - Using student/staff biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise students.

- **Special category data**: Personal data which the GDPR says is more sensitive, and so needs more protection – where biometric data is used for identification purposes, it is considered special category data.

4. ROLES AND RESPONSIBILITIES

The Governing Body (PPM Committee) is responsible for:

- Reviewing this policy every two years.

- The Headteacher/Business Manager is responsible for:

- Ensuring the provisions in this policy are implemented consistently.

- The Data Protection Officer (DPO)/Deputy DPO is responsible for:

- Monitoring the school's compliance with data protection legislation in relation to the use of biometric data.
- Advising on when it is necessary to undertake a Data Protection Impact Assessment (DPIA) in relation to the school's biometric system(s).
- Being the first point of contact for the ICO and for individuals whose data is processed by the school and connected third parties.

5. DATA PROTECTION PRINCIPLES

- The school processes all personal data, including biometric data, in accordance with the key principles set out in the GDPR.

- The school ensures biometric data is:

- Processed lawfully, fairly and in a transparent manner.
- Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- As the Data Controller, the school is responsible for being able to demonstrate its compliance with the provisions outlined above.

6. DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

- Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out.

- The DPO will oversee and monitor the process of carrying out the DPIA.

- The DPIA will:

- Describe the nature, scope, context and purposes of the processing.
- Assess necessity, proportionality and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.

- When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered.

- If a high risk is identified that cannot be mitigated, the DPO will consult the ICO before the processing of the biometric data begins.

- The ICO will provide the school with a written response (within eight weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether the school needs to take further action. In some cases, the ICO may advise the school to not carry out the processing.

- The school will adhere to any advice from the ICO.

7. PROVIDING YOUR CONSENT/OBJECTING

Please note that the obligation to obtain consent for the processing of biometric information of children under the age of 18 is not imposed by the Data Protection Act 2018 or the GDPR. Instead, the consent requirements for biometric information is imposed by Section 26 of the Protection of Freedoms Act 2012.

Where the school uses student and staff biometric data as part of an automated biometric recognition system (e.g. using students' fingerprints to receive school dinners instead of paying with cash), the school will comply with the requirements of the Protection of Freedoms Act 2012.

Written consent will be sought from at least one parent/carer of the student before the School collects or uses a student's biometric data.

The name and contact details of the student's parent/carers will be taken from the school's admission register.

Where the name of only one parent/carer is included on the admissions register, the Headteacher will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent/carer.

The school does not need to notify a particular parent/carer or seek their consent if it is satisfied that:

- The parent/carer cannot be found, e.g. their whereabouts or identity is not known.
- The parent/carer lacks the mental capacity to object or consent.
- The welfare of the student requires that a particular parent/carer is not contacted, e.g. where a student has been separated from an abusive parent/carer who must not be informed of the student's whereabouts.
- It is otherwise not reasonably practicable for a particular parent/carer to be notified or for their consent to be obtained.

Notification sent to parent/carers and other appropriate individuals or agencies will include information regarding the following:

- Details about the type of biometric information to be taken.
- How the data will be used.
- The parent/carer's and the student's right to refuse or withdraw their consent.
- The school's duty to provide reasonable alternative arrangements for those students whose information cannot be processed

The school will not process the biometric data of a student under the age of 18 in the following circumstances:

- The student (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data.
- No parent/carer or carer has consented in writing to the processing.

- A parent/carer has objected in writing to such processing, even if another parent/carer has given written consent.

Parent/carers and students can object to participation in the school's biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the student that has already been captured will be deleted.

If a student objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the trust will ensure that the student's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the student's parent/carer(s).

Where staff members or other adults use the school`s biometric system(s), consent will be obtained from them before they use the system.

Staff and other adults can object to taking part in the school's biometric system(s) and can withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

Alternative arrangements will be provided to any individual that does not consent to take part in the school`s biometric system(s), in line with section 8 of this policy.

8. ALTERNATIVE ARRANGEMENTS

Where an individual objects to taking part in the school's biometric system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service, e.g. where a biometric system uses student's fingerprints to pay for school meals, the student will be able to use ~~cash~~ a pin code for the transaction instead.

Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service.

9. DATA RETENTION

Biometric data will be managed and retained in line with the school's Records Management Policy.

If an individual (or a student's parent/carer, where relevant) withdraws their consent for their/their child's biometric data to be processed, it will be erased from the school's system.

10. MONITORING AND REVIEW

The Governing Body will review this policy every two years. The updated policy will be made available to all staff, parent/carers and students on the school website.

Please note that, when your child leaves the school or ceases to use the biometric system, their biometric information will be securely erased in line with the school's Records Management Policy.

11. FURTHER INFORMATION AND GUIDANCE

This can be found via the following links:

Department for Education's 'Protection of Biometric Information of Children in Schools – Advice for proprietors, governing bodies, head teachers, principals and school staff:

https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

ICO guidance on data protection for education establishments:

https://ico.org.uk/for-organisations/in-your-sector/education/

12. FREQUENTLY ASKED QUESTIONS

What information should schools provide to parents/carers/students to help them decide whether to object or for parents/carers to give their consent?

Any objection or consent by a parent/carer must be an informed decision – as should any objection on the part of a child. Schools and colleges should take steps to ensure parents/carers receive full information about the processing of their child's biometric data including a description of the kind of system they plan to use, the nature of the data they process, the purpose of the processing and how the data will be obtained and used. Children should be provided with information in a manner that is appropriate to their age and understanding.

What if one parent disagrees with the other?

Schools and colleges will be required to notify each parent/carer of a child whose biometric information they wish to collect/use. If one parent/carer objects in writing, the school or college will not be permitted to take or use that child's biometric data.

How will the child's right to object work in practice – must they do so in writing?

A child is not required to object in writing. An older child may be more able to say that they object to the processing of their biometric data. A younger child may show reluctance to take part in the physical process of giving the data in other ways. In either case, the school or college will not be permitted to collect or process the data.

Are schools required to ask/tell parents/carers before introducing an automated biometric recognition system?

Schools are not required by law to consult parents/carers before installing an automated biometric recognition system. However, they are required to notify parents/carers and secure consent from at least one parent/carer before biometric data is obtained or used for the purposes of such a system. It is up to schools to consider whether it is appropriate to consult parents/carers and students in advance of introducing such a system.

Do schools need to renew consent every year?

No. The original written consent is valid until such time as it is withdrawn. However, it can be overridden, at any time if another parent/carer or the child objects to the processing (subject to the parent/carer's objection being in writing). When the student leaves the school, their biometric data should be securely removed from the school's biometric recognition system.

Do schools need to notify and obtain consent when the school introduces an additional, different type of automated biometric recognition system?

Yes, consent must be informed consent. If, for example, a school has obtained consent for a fingerprint/fingertip system for catering services and then later introduces a system for accessing library services using iris or retina scanning, then school will have to meet the notification and consent requirements for the new system.

Can consent be withdrawn by a parent/carer?

Parents/carers will be able to withdraw their consent, in writing, at any time. In addition, either parent/carer will be able to object to the processing at any time but they must do so in writing.

When and how can a child object?

A child can object to the processing of their biometric data or refuse to take part at any stage – i.e. before the processing takes place or at any point after his or her biometric data has been obtained and is being used as part of a biometric recognition system. If a student objects, the school or college must not start to process his or her biometric data or, if they are already doing this, must stop. The child does not have to object in writing.

Will consent given on entry to primary or secondary school be valid until the child leaves that school?

Yes. Consent will be valid until the child leaves the school – subject to any subsequent objection to the processing of the biometric data by the child or a written objection from a parent/carer. If any such objection is made, the biometric data should not be processed and the school or college must, in accordance with the GDPR, remove it from the school's system by secure deletion.

Can the school notify parents and accept consent via email?

Yes – as long as the school is satisfied that the email contact details are accurate and the consent received is genuine.

Will parents/carers be asked for retrospective consent?

No. Any processing that has taken place prior to the provisions in the Protection of Freedoms Act coming into force will not be affected. Any school or college wishing to continue to process biometric data must have already sent the necessary notifications to each parent/carer of a child and obtained the written consent from at least one of them before continuing to use their child's biometric data.

Does the legislation cover other technologies such a palm and iris scanning?

Yes. The legislation covers ***all*** systems that record or use physical or behavioural characteristics for the purpose of identification. This includes systems which use palm, iris or face recognition, as well as fingerprints.

Is parental notification and consent required under the Protection of Freedoms Act 2012 for the use of photographs and CCTV in schools?

No – not unless the use of photographs and CCTV is for the purposes of an automated biometric recognition system. However, schools and colleges must continue to comply with the requirements in the GDPR when using CCTV for general security purposes or when using photographs of students as part of a manual ID system or an automated system that uses barcodes to provide services to students. Depending on the activity concerned, consent may be required under the GDPR before personal data is processed.

The Government believes that the GDPR requirements are sufficient to regulate the use of CCTV and photographs for purposes other than automated biometric recognition systems. Photo ID card systems, where a student's photo is scanned automatically to provide them with services, would come within the obligations on schools and colleges under sections 26 to 28 of the Protection of Freedoms Act 2012, as such systems fall within the definition in that Act of automated biometric recognition systems.

Is parental/carer notification or consent required if a student uses or accesses standard commercial sites or software which use face recognition technology?

The provisions in the Protection of Freedoms Act 2012 only cover processing by or on behalf of a school or college. If a school or college wishes to use such software for school work or any school business, the requirement to notify parents/carers and to obtain written consent will apply. However, if a student is using this software for their own personal purposes, the provisions do not apply, even if the software is accessed using school or college equipment.

LINKED POLICIES:

- Data Retention Policy
- Freedom of Information Policy

Appendix I

CCTV SYSTEM ANNUAL REVIEW

Kirkbie Kendal School has considered the need for CCTV monitoring and has decided it is necessary for the prevention and detection of crime and for the personal protection of our staff, students, visitors and other members of our community and ensuring that site rules are respected so that the school can be properly managed. It will not be used for other purposes. We conduct an annual review of our use of CCTV as follows.

School/Setting:		**Date:**	
Assessor:		**Signed:**	

Review Statement	Satisfactory		Problems Identified *(if any)*	Corrective Action Required *(if relevant)*	Completed By	Date Complete
	Yes	No				
Notification has been submitted to the Information Commissioner's Office and the next renewal date recorded.						
There is a named individual who is responsible for operation of the system.						
The problem we are trying to address has been clearly defined and installing cameras is the best solution.						
The CCTV system is addressing the needs and delivering the benefits that justified its use.						
The system equipment produces clear images which law enforcement (usually the police) can use to investigate crime and these can easily be taken from the system when required.						
Cameras have been sited so that they provide clear images.						
Cameras have been positioned to avoid capturing images of people who are not visiting the premises.						
There is sufficient suitable signage notifying people that CCTV monitoring is in operation, including our contact details where it might not be obvious that the system is managed by this school.						
Information is available to help deal with queries about operation of the system and how individuals can make access requests.						
Sufficient safeguards are in place to protect wireless transmission systems from interception.						

Appendix I

Review Statement	Satisfactory		Problems Identified *(if any)*	Corrective Action Required *(if relevant)*	Completed By	Date Complete
	Yes	No				
There are sufficient controls and safeguards in place if the system is connected to, or made available across, a computer, e.g. an intranet.						
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.						
The ability to make copies of recorded data is restricted to appropriate staff.						
Recorded data will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.						
The process for deleting data is effective and being adhered to.						
Except under the direction of an appropriate public authority (usually law enforcement), images will not be provided to third parties.						
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.						
We know how to respond to individuals making requests for copies of their own images and if we are unsure we know how to seek advice from the Information Commissioner as soon as such a request is made.						
When information is disclosed, it is transmitted as securely as possible e.g. hand delivered/collected in person on a device, a fully tracked postal service etc.						
Staff are trained in security procedures and there are sanctions in place for any misuse of surveillance system information.						
Staff have been made aware that they could be committing a criminal offence if they misuse surveillance system information.						
Regular checks are carried out to ensure that the system is working properly and produces high quality and useful data.						
There is a system in place to ensure that any manufacturer recommended CCTV system and equipment updates, especially of security software are regularly sought, applied and checked as properly functioning.						

Appendix I

Review Statement	Satisfactory		Problems Identified *(if any)*	Corrective Action Required *(if relevant)*	Completed By	Date Complete
	Yes	No				
Please keep this checklist in a safe place until the date of the next Annual Review.						

Guiding Principles of the Surveillance Camera Code of Practice

System operators should adopt the following 12 guiding principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

Source: *The Information Commissioner's Office 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data, June 2017 (Appendix 3)*

Appendix G - CCTV Procedures

Appendix F - Biometric Data

Data Classifications and Handling Requirements

This is an indicative rather than exhaustive guide to data classification and the resulting data handling requirements. All relevant queries should be directed to the Data Protection Officer or the Data Protection Support Assistant or the Information Technology Manager [insert names and contact details].

	Public	Confidential	Sensitive
Impact if the information becomes public	**No risk**	**Low-Medium Risk** May result in minor reputational or financial damage to the school. May result in minor privacy breach for an individual.	**Medium-High Risk** Could substantially damage the reputation of the school, have a substantial financial effect on school or a third party, or would result in a serious privacy breach to one or more individuals.
Description of the information	Information that does not require protection and is considered "open and unclassified" and which may be seen by anyone whether directly linked with school or not. Information is likely to already exist in the public domain.	May result in minor reputational or financial damage to the school. May result in a minor privacy breach for an individual. Information that should only be available to sub-groups of staff within the school who need the information to carry out their roles.	Information that has the potential to cause serious damage or distress to individuals or serious damage to the school's interests if disclosed inappropriately. Information which is sensitive in some way because it might be sensitive personal data, commercially sensitive, legally privileged or under embargo. This information should only be available to a small tightly restricted group of authorised users.
Examples of information This list is indicative not exhaustive if unsure ask name/role for advice	● Prospectus ● Press releases ● Open content on the school web site ● Publicity flyers and leaflets ● Published information released under the Freedom of Information Act ● Policies, annual reports and financial statements ● Job adverts (excluding internal only positions) ● staff names and contact details ● Staff publications. ● Agendas and minutes of school committees and working groups (except reserved business). ● Patented intellectual property.	● Student personal details e.g. demographics, personal email address etc. ● Staff personal details e.g. demographic, payroll number, personal email address etc. ● Internal only school policies, processes and guidelines. ● Internal only job adverts. ● Tender bids prior to award of contract ● Individual's salaries ● Student's assessment marks. ● Job application responses/CVs (unless they contain sensitive personal information).	Sensitive personal data and some other data. ● Exam questions prior to use ● Medical records ● UPRNs ● Usernames and passwords ● Investigations/disciplinary proceedings. ● Payment card details. ● Financial information (banking details and data not already disclosed in financial statements). ● Passwords and access codes to school systems. ● Some complaints or requests ● Biometric data
Security Marking	No marking required	Must be clearly marked as **Confidential**	Must be clearly marked as **Sensitive**

	Public	Confidential	Sensitive
Storage (electronic)	● Store using school IT facilities to ensure appropriate management, back-up and access. ● Use only the school approved cloud service [insert name here]. Some cloud services may **not** be used because they link to computer C: drives which is not secure.	● Store only on the school IT network and never on the C: drive of a PC/laptop (beware downloading information when a laptop is not connected to the school domain - the download will go onto the C: drive and you may be in breach of this policy). ● Store only on the C: drive of a specially encrypted PC/laptop. ● Store only on the approved cloud service in a suitably restricted folder. ● Portable devices such as USB sticks must be encrypted and must **not** be used for long term storage due to the risks of loss or corruption of data. ● Never to be stored on any personal device or personal cloud service not controlled by school or on any unencrypted school device e.g. tablet, laptop, mobile phone etc.	● Store only on the school IT network in rigorously monitored & restricted access drives. ● Never to be stored on the approved cloud service unless also separately encrypted. ● Never to be stored on any portable storage device i.e. USB drive regardless of encryption. ● Never to be stored on any personal device or personal cloud service not controlled by school or on any school device e.g. tablet, laptop, mobile phone etc. unless it has been specially encrypted *and* there are other high level procedural safeguards.
School Website	No restrictions	Not permitted	Not permitted
Storage (hardcopy)	No restrictions	In a lockable cabinet/drawer which is locked when unattended and where the room is also locked when unoccupied. If not in a lockable store the room where this classification of data is kept should be locked at all times when unattended and must have restricted access.	In a lockable cabinet/drawer which is locked when unattended and where the room is also locked when unoccupied. If not in a lockable store the room where this classification of data is kept should be locked at all times when unattended and must have restricted access.
Email hosted by school	No restrictions	Emails to external recipients must not contain this data. It must be an encrypted email or sent as an encrypted attachment and the password conveyed by a separate mechanism e.g. telephone. Emails to internal recipients i.e. school email account-to-school email account are secure, so encryption and encrypted attachments are not necessary.	Emails to external recipients must not contain this data. It must be an encrypted email or sent as an encrypted attachment and the password conveyed by a separate mechanism e.g. telephone. Emails to internal recipients i.e. school email account-to-school email account are secure, so encryption and encrypted attachments are not necessary.
Personal email account e.g. Hotmail etc.	No restrictions	Not permitted	Not permitted
Post (Internal)	No restrictions	In a sealed envelope marked Confidential.	Seal envelope, mark Confidential & hand deliver.

	Public	Confidential	Sensitive
Post (External)	No restrictions	Tracked and recorded delivery only and marked Confidential	Tracked and recorded delivery only and marked Confidential within two separate envelopes.
School-based server	No restrictions but consideration should be given to back-up requirements.	No storage or creation is permitted unless the server environment is equivalent to the school-based server or the CTU server environment.	No storage or creation permitted unless the server environment is equivalent to the school-based server or the CTU server environment.
School owned laptop	No restrictions but do **not** use to store master copies of vital records.	The internal storage (hard drive(s), HDDs, SSDs) must be encrypted and set to lock after five minutes of inactivity.	The internal storage (hard drive(s), HDDs, SSDs) must be encrypted and set to lock after five minutes of inactivity.
Personally owned mobile device	No restrictions	Only to be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with the ICO BYOD guidance document.	Not permitted unless authorised by the Senior Information Risk Owner (SIRO). Only then to be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with the ICO BYOD guidance document.
School owned desktop (public areas)	No restrictions, but always lock the screen when unattended.	Not permitted. The risk of incidental disclosure is too high.	Not permitted. The risk of incidental disclosure is too high.
School owned desktop (key/card access controlled areas)	No restrictions, but always lock the screen when unattended.	Only permitted on encrypted drives or using or password protected files. Always lock the screen when unattended.	Only permitted on encrypted drives. Always lock the screen when unattended.
School owned mobile device	No restrictions, but always lock the screen when unattended.	Only to be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with our policy and the ICO BYOD guidance document.	Not permitted unless authorised by the SIRO. Only then to be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with our policy and the ICO BYOD guidance document
Removable media (CDs, USB drives etc.)	No restrictions.	Encrypted storage with strong password e.g. 8 characters or longer and a mixture of uppercase, lowercase, digits and special characters.	Encrypted storage with strong password e.g. 8 characters or longer and a mixture of uppercase, lowercase, digits and special characters.
Disposal	No restrictions. Recycle where possible.	Shred or place in a confidential waste bag. Delete from electronic media when no longer required.	Cross shred only & put shredded material into the confidential waste. Appropriately scrub data from devices. Some devices (encrypted USB drives) may need to be securely destroyed. Seek advice from the IT manager.