Data Protection Policy

(previously included in Data Protection and Information Management Policy)

Version 1

Important: This document can only be considered valid when viewed on the Trust website. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.	
Author	COO
Name of Responsible Committee / Individual	Trust Board
Target Audience	All Stakeholders
Date Policy Agreed	October 2026
Review Date	September 2027
Related Documents	Acceptable Use Policy Information Security Policy Freedom of Information Act 2000 Publication Scheme FOI Policy CCTV Policy Records Management Policy
References	www.cio.org.uk

Contents

Introduction and Scope 3
Roles and Responsibilities 3
Data Protection Principles 4
Lawful Bases 5
Data Subject Rights 5
Records of Processing 6
Privacy by Design and Risk Assessments 7
Information Sharing 7
Contract Management 7
Training 8
Data Protection Complaints 8
Appendix 1 – Appropriate Policy Document (APD) 9
Appendix 2 – Subject Access Requests (SAR) 13
Appendix 3 – Freedom of Information (FOI) and Environmental Information Regulation (EIR) Requests 15
Appendix 4 – Surveillance 18
Appendix A – Surveillance Camera System Checklist 21
Appendix 5 – Biometrics 23

Introduction and Scope

Brighter Futures Learning Partnership Trust is required to process personal information about staff, pupils, parents, guardians, and other individuals we may interact with. We must do this in compliance with data protection and other relevant legislation.

This policy provides a framework for ensuring that we comply with the requirements of the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA), and other relevant legislation, as well as associated guidance and codes of practice.

This policy, including its appendices, applies to our entire workforce. This includes employees, governors or trustees, contractors, agents and representatives, volunteers and temporary staff working for or on our behalf. Individuals found to knowingly or recklessly infringe this policy may face disciplinary action.

This is our main information governance policy and applies to all personal data, whether paper or electronic. It should be read alongside the other policies within our information governance policy framework.

Roles and Responsibilities

Overall responsibility for ensuring that we meet the statutory requirements of any data protection legislation lies with the Board of Governors or Trustees. The following roles will have day-to-day responsibility for compliance and providing the necessary assurance to the Board.

Data Protection Officer (DPO)

The role of the DPO is to assist us in monitoring compliance with data protection legislation and advise on data protection issues. We have appointed Veritau as our DPO. Veritau's contact details are:

Schools Data Protection Officer
Veritau
West Offices
Station Rise
York
North Yorkshire
YO1 6GA

schoolsdpo@veritau.co.uk // 01904 554025

The DPO is an advisory role, and its duties include:

- Informing and advising us and our employees about our obligations to comply with the UK GDPR, the Data Protection Act 2018, and other data protection and information access laws;
- Monitoring compliance with data protection legislation and other information governance policies;
- Raising awareness of data protection issues; and
- Liaising with the Information Commissioner's Office (ICO).

Senior Information Risk Owner (SIRO)

The SIRO is a senior staff member who is ultimately responsible for information risk. The SIRO will ensure that our information governance policies and procedures are effective and comply with legislation, promote best practice, and embed a culture of data protection compliance. In our organisation, this role lies with the Chief Executive Officer.

Single Point of Contact (SPOC)

The SPOC will take operational responsibility for data protection compliance, including communicating with data subjects and the DPO. In our organisation, this role lies with the Chief Operating Officer.

Information Asset Owner (IAO)

An IAO is an individual responsible for the security and maintenance of a particular information asset and for ensuring that other staff members use the information safely and responsibly. IAOs will be appointed based on sufficient seniority and level of responsibility and will be documented in our Information Asset Register (IAR).

All staff

All staff, including governors or trustees, contractors, agents and representatives, volunteers, and temporary staff working for or on our behalf, will be responsible for collecting, storing, and processing personal data in accordance with this policy.

Data Protection Principles

We will comply with the data protection principles defined in Article 5 of the UK GDPR. We will ensure that personal information is:

- Processed lawfully, fairly and transparently **(Lawfulness, Fairness and Transparency)**.
- Collected only for specified, explicit, and legitimate purposes **(Purpose Limitation)**.
- Adequate, relevant, and limited to what is necessary for the purposes for which it is processed **(Data Minimisation)**.
- Accurate and, where necessary, kept up to date **(Accuracy)**.

- Not kept in a form that permits identification of data subjects for longer than is necessary for the purposes for which the data is processed **(Storage Limitation)**.
- Processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage **(Security, Integrity and Confidentiality)**.

We recognise that we must comply with the above principles and be able to demonstrate our compliance **(Accountability).**

Lawful Bases

UK GDPR sets out several conditions for lawfully processing personal information. We will usually rely on the lawful basis of public task or legal obligation; however, we may sometimes rely on our legitimate interests. We will only do this where we use data in ways individuals would reasonably expect and where we have a justifiable reason.

When relying on our legitimate interests, we will ensure that we provide individuals with clear and transparent information about how personal data will be used, including details on how to opt-out.

We may rely on vital interests as the lawful basis for sharing information in a situation where we believe someone is at risk of serious harm, for example, in a mental health emergency.

We will have an Appropriate Policy Document (APD) in place (see Appendix One) that provides information about our processing of special category (SC) and criminal offence (CO) data and demonstrates how we comply with the requirements of the UK GDPR and DPA.

Data Subject Rights

Under the UK GDPR, individuals have several rights in relation to the processing of their personal data:

Right to be informed

When we collect their data, we will provide individuals with privacy information, normally through a privacy notice made easily accessible to the data subject. Privacy notices will be clear and transparent, regularly reviewed, and include all information required by data protection legislation.

Right of access

Individuals have the right to access and receive a copy of the information we hold about them. This is commonly known as a subject access request (SAR). We will have a SAR procedure that details how we deal with these requests (Appendix Two).

Other rights include the right to rectification, right to erasure, right to restrict processing, right to object, right to data portability and rights related to automated decision-making, including profiling.

Requests exercising these rights can be made to any staff member. Still, we encourage requests to be made in writing, wherever possible, and forwarded to the SPOC, who will acknowledge the request and respond within one calendar month. Advice regarding such requests will be sought from our DPO where necessary.

A record of decisions made regarding the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision.

Records of Processing

Under Article 30 of the UK GDPR, we must record our processing activities. We will do this by developing and maintaining an Information Asset Register (IAR), which will include, as a minimum:

- The organisation's name and contact details
- The name of the information asset
- The owner of that asset, known as the Information Asset Owner (IAO)
- The purposes of the processing
- A description of the categories of individuals and the types of personal data
- Who has access to the personal data, and who it is shared with
- The lawful basis for each processing activity
- The format and location of the personal data
- Details of any transfers to countries outside of the UK and the appropriate safeguards
- The retention periods for each asset
- A general description of the technical and organisational security measures to protect the information.

We review the IAR at least annually to ensure it remains accurate and up to date, consulting with the DPO as necessary.

Privacy by Design and Risk Assessments

We will adopt privacy by design and implement appropriate technical and organisational security measures to demonstrate how we will integrate data protection into our processing activities.

We will conduct a data protection impact assessment (DPIA) when undertaking new, high-risk processing or making significant changes to existing data processing. The DPIA will consider and document the risks associated with a project before its implementation, ensuring data protection is embedded by design and default.

The data protection principles will be assessed to identify specific risks. These risks will be evaluated, and solutions to mitigate or eliminate them will be considered. Where a less privacy-intrusive alternative is available, or the project can go ahead without the use of special category data, we will opt to do this.

Information Sharing

Sometimes, we must share information with third parties to effectively fulfil our duty of education provision. Our privacy notices and IAR will document routine and regular information-sharing arrangements.

Any further or ad-hoc information sharing will only be done in compliance with legislative requirements, including the ICO's data-sharing code of practice. We will only share personal information where we have a lawful basis, ensuring any disclosure is necessary and proportionate. All disclosures will be approved by the relevant staff member and recorded in a disclosure log.

Contract Management

All third-party providers who process data on our behalf must be able to provide assurances that they have adequate data protection controls in place. Where personal data is being processed, we will ensure that a written contract includes all the mandatory data processing clauses in accordance with Article 28 of the UK GDPR.

We will maintain a record of our data processors and regularly review the data processing contracts, with support from the DPO, to ensure continued compliance.

Where possible, personal information we process is not transferred outside of the European Economic Area (EEA), which the UK government deems to have adequate data protection standards. If personal data is transferred outside the EEA, we will consult with the DPO and take reasonable steps to ensure appropriate safeguards are in place. These safeguards will be recorded in our data processor register.

Training

We will ensure that appropriate guidance and training on data protection and access to information are given to our workforce, governors or trustees, and other authorised users. Training will be delivered as part of the induction process and at least every two years. Refresher training will be carried out as required.

Specialised roles or functions with key data protection responsibilities, such as the SIRO, SPOC and IAOs, will also receive additional training specific to their role.

We will maintain a record of all completed training and ensure that data protection awareness is raised in staff briefings and as standard agenda items in meetings, where appropriate.

Data Protection Complaints

Data protection complaints relating to a completed SAR will be processed as an internal review request in accordance with Appendix 2.

Any other complaints or concerns about our compliance with data protection legislation or our handling of personal data will be dealt with as a data protection complaint.

Our general data protection complaints procedure is as follows:

- Complaints may be received directly by email, telephone, or in person. Alternatively, individuals may contact our Data Protection Officer.
- We encourage individuals to provide sufficient evidence or supporting information where possible, to allow us to investigate the complaint.
- If necessary, we may request proof of ID (or proof of authority where the complainant is acting on behalf of another person).
- We will acknowledge complaints within 30 days of receipt. This includes weekends and bank holidays.
- We will take steps to respond to complaints without undue delay. This includes making appropriate enquiries and keeping the complainant informed.
- We will inform people of the outcome of their complaints. This includes explaining any steps we have taken to address the complaint.

If an individual remains dissatisfied after we have concluded our internal data protection complaints process, they may complain to the Information Commissioner's Office. Its contact details are below:

The telephone helpline (0303 123 1113) is open Monday to Friday between 9 a.m. and 5 p.m. (excluding bank holidays). Alternative methods for reporting, enquiring, registering, and raising complaints are available on the ICO's website here.

Appendix 1 – Appropriate Policy Document (APD)

Introduction

Brighter Futures Learning Partnership Trust processes special category and criminal conviction data while fulfilling its functions. Schedule 1 of the Data Protection Act 2018 requires data controllers to have an 'appropriate policy document' where certain processing conditions apply for special categories of personal and criminal conviction data. This document will fulfil this requirement.

This will complement our existing records of processing as required by Article 30 of the UK General Data Protection Regulation. It will also reinforce our existing retention and security policies, procedures, and other documentation regarding special category data.

Special categories and conditions of processing

We will process the following special categories (SC) of data:

- racial or ethnic origin
- religious or philosophical beliefs
- trade union membership
- health or medical information
- sex life and sexual orientation
- biometric identifiers

We will also process criminal offence (CO) data under Article 10 of the UK GDPR, including pre-employment checks and employee declarations, in accordance with their contractual obligations.

We will rely on the following processing conditions under Article 9 of UK GDPR and Schedule 1 of the Data Protection Act 2018 to process special category and criminal convictions data lawfully:

Article 9(2)(a) – explicit consent

We will ensure that consent obtained from individuals is clear and specific for one or more outlined purposes. It must be granted through affirmative action and recorded as a requirement for processing. We will also conduct regular reviews of consents to ensure they remain current and valid.

Examples of such processing include asking visitors for health or medical information to aid them in an emergency or using biometric (fingerprint) data for identification or authentication purposes for school meal payments.

Article 9(2)(b) – employment, social security or social protection
We must collect special category data to comply with our legal requirements as an employer and safeguard our pupils.

Examples include carrying out DBS checks on staff to evidence suitability for a role, collecting medical information to make reasonable adjustments at work and monitor staff absence, and keeping records of an employee's trade union membership.

When processing information under Article 9(2)(b), we also require a Schedule 1 condition under the Data Protection Act 2018. The condition we will rely on for this processing is **Schedule 1, Part 1, (1) - employment, social security and social protection.**

Article 9(2)(c) – vital interest
We must share SC data where an individual is physically or legally unable to consent and there is a serious risk to life.

An example is when there is an urgent or emergency situation, and an individual is at risk of harm to themselves or to others, such as in a mental health crisis.

A Schedule 1 condition is not required for processing under Article 9(2)(c).

Article 9(2)(g) – reasons of substantial public interest
Much of our processing of SC data will be done so for the purposes of substantial public interest.

Examples include processing SC data to identify pupils who require additional support, such as special educational needs, processing safeguarding concerns to ensure the safety and well-being of pupils, or collecting medical information when monitoring pupil attendance and allergen or dietary requirements.

When processing data under Article 9(2)(g), we also require a Schedule 1 condition under the Data Protection Act 2018. The conditions we will rely on for this processing are **Schedule 1, Part 2, (6) – statutory and government purposes; (10) – preventing or detecting unlawful acts; and (18) – safeguarding of children and of individuals at risk.**

Compliance with data protection principles
We will have several policies and procedures in place to ensure our compliance with the Article 5 data protection principles and meet our accountability obligations:

Accountability principle
We will implement appropriate technical and organisational security measures to meet the accountability requirements. These will include:

- The appointment of a Data Protection Officer.
- Taking a data protection by design and default approach to our processing activities, including completing risk assessments.
- Maintaining documentation of our processing activities through an Information Asset Register.
- Adopting and implementing an information governance framework.
- Ensuring we have compliant contracts in place with data processors.
- Implementing appropriate security measures regarding the personal data we process. Our Information Security Policy provides more detail.

Principle (a): lawfulness, fairness and transparency
Processing personal data must be lawful, fair and transparent. We will identify an appropriate Article 6 condition and, where processing SC or CO data, an Article 9 and Schedule 1 condition.

We will consider how processing may affect individuals concerned and provide clear and transparent information about why we process personal data, including our lawful bases, in our privacy notices and this document. All privacy notices will provide details of data subject rights. Our privacy information will be regularly reviewed and updated to reflect our processing accurately.

Principle (b): purpose limitation
Organisations can only act in ways and for purposes for which they are empowered to do so by law. Personal data is, therefore, only processed to allow us to carry out the necessary functions and services we are required to provide in line with legislation.

We will clearly set out our purposes for processing in our privacy notices, policies and procedures, and in our IAR. If we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we will check that it is compatible with our original purpose, or we will advise individuals of the new purpose.

Principle (c): data minimisation
We will only collect the minimum personal data needed for the relevant purposes, ensuring it is necessary and proportionate. Any personal information no longer required, especially with special category data, will be anonymised or erased. Further information can be found in our Records Management Policy.

Principle (d): accuracy
When we become aware that personal data is inaccurate or outdated, we will take reasonable steps to ensure that data is erased or rectified without delay. Where we cannot erase or rectify the data, for example, because the lawful basis we rely on to process the data means these rights do not apply, we will document our decision.

Where we have shared information with a third party, we will take reasonable steps to inform them of the inaccuracies and rectification. We will maintain a log of all data rights requests and have appropriate processes for handling such requests.

Principle (e): storage limitation

Our retention schedule will set out how long we will retain records. Where there is no legislative or best practice guidance, the SIRO will decide how long the information should be retained based on its necessity for legitimate purposes. We will also maintain a destruction log, documenting what information was destroyed, the date it was destroyed, and why. Further information can be found in our Records Management Policy.

Principle (f): integrity and confidentiality (security)

We will employ various technical and organisational security measures to protect the personal and special category data that we process. A full description of security measures can be found in our Information Security Policy.

In the event of a personal data breach, the incident will be recorded on a log, investigated, and reported to our Data Protection Officer where necessary. This process is documented in greater detail in our Information Security Policy.

Appendix 2 – Subject Access Requests (SAR)

Under the UK GDPR, individuals have the right to make a subject access request (SAR) to any member of our workforce, governor or trustee, contractor or agent working on our behalf. Requests need not be made in writing, but we will encourage applicants to do so where possible. Requests should be forwarded to the SPOC who will log and acknowledge them within five working days.

We must be satisfied with the requestor's identity and may have to ask for additional information to verify this, such as:

- valid photo ID, such as driver's licence or passport
- proof of address, such as a utility bill or council tax letter
- confirmation of email address.

Only once we are confident of the requestor's identity and have sufficient information to understand the request will it be considered valid. We will then respond to the request within the statutory timescale of one calendar month.

If the request is considered 'complex', we can apply a discretionary extension of up to two more calendar months. If we wish to apply an extension, we will inform the applicant within the first calendar month of receiving the request.

Requests are considered 'complex' only if we can demonstrate that they meet one or more of the following factors:

- Information is technically difficult to retrieve, or specialist support is required.
- Large volumes of sensitive information where exemptions may need to be applied.
- Clarifying potential issues concerning confidentiality and/or disclosure of sensitive information.
- Needing to obtain specialist legal advice.
- Searching large volumes of unstructured manual records.

Requests involving large volumes of information may add complexity, but volume alone is not considered 'complex.'

If we consider applying exemptions to the requested information before disclosure, we will seek guidance from our DPO. We may also refuse a manifestly unreasonable or excessive request in limited circumstances.

For Trust secondary settings only:
If a parent whose child is 12 years or over makes a subject access request, we may consult with the child, ask that they submit the request on their own behalf, or confirm permission for the disclosure. This decision will be made based on the pupil's capacity to understand the request and disclosure risks.

Internal review
Data protection complaints related to completed SARs will be processed as internal review requests.

When acknowledging receipt, we will inform you that we are processing your complaint as an internal review request.

An internal review will be handled by an appropriate staff member who was not involved in the original request. They will examine the original request and response and decide whether it was handled appropriately and whether it followed the legislation. The reviewing officer will decide whether to uphold or overturn any exemptions. Where possible, a full response will be provided within one calendar month.

If an individual remains dissatisfied after our investigation, they may appeal to the Information Commissioner's Office. Its contact details are below:

The telephone helpline (0303 123 1113) is open Monday to Friday between 9 a.m. and 5 p.m. (excluding bank holidays). Alternative methods for reporting, enquiring, registering, and raising complaints are available on the ICO's website here.

Appendix 3 – Freedom of Information (FOI) and Environmental Information Regulation (EIR) Requests

Freedom of Information (FOI)

The Freedom of Information Act 2000 (FOIA) is part of the Government's commitment to greater openness and transparency in the public sector. It enables members of the public to scrutinise the decisions of public authorities more closely and ensure that services are delivered properly and efficiently. Public authorities have two main responsibilities under the Freedom of Information Act:

- To publish certain information about its activities in a publication scheme, and
- To process and respond to individual requests for information, with a duty to provide advice and assistance.

Under FOI, anyone can request access to the recorded information we hold. Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings. A code of practice under section 45 of the Act sets out recommendations for handling requests for information. To comply with this code, requests must:

- Be in writing
- Provide the name or company name and contact or email address
- Describe the information being requested
- Ideally, state the preferred format they would like the information to be provided.

Any request that cannot be answered promptly as part of normal day-to-day business or where we are asked to handle it under Freedom of Information will be treated as an FOI request.

Information can be withheld if one or more of the 24 exemptions within the FOIA apply. This could mean that certain information is not released in response to a request or is not published. Requests for information can be refused for reasons including:

- The information is not held
- It would cost too much or take too much staff time to comply with the request
- The request is considered vexatious
- The request repeats a previous request from the same person.

Environmental Information Regulations (EIR)

Requests for information related to the environment, including activities that may affect the environment, will be handled under the Environmental Information Regulations 2004. EIR is similar to FOI, but there is an even greater presumption of disclosure and fewer exceptions under which a request can be refused. Requests under EIR can also be given verbally and do not need to be in writing, but must include:

- A name or company name and contact or email address
- A description of the information being requested

- Ideally, state the preferred format they would like the information to be provided.

'Environmental information' includes information which relates to:

a) the state of the elements of the environment, such as air and atmosphere, water, soil, land, landscape and natural sites, including wetlands, coastal and marine areas, biological diversity and its components, including genetically modified organisms, and the interaction among these elements
b) factors such as substances, energy, noise, radiation or waste, including radioactive waste, emissions, discharges and other releases into the environment, affecting or likely to affect the elements of the environment referred to in (a)
c) measures (including administrative measures), such as policies, legislation, plans, programmes, environmental agreements, and activities affecting or likely to affect the elements and factors referred to in (a) and (b), as well as measures or activities designed to protect those elements
d) reports on the implementation of environmental legislation
e) cost-benefit and other economic analyses and assumptions used within the framework of the measures and activities referred to in (c)
f) the state of human health and safety, including the contamination of the food chain, where relevant, conditions of human life, cultural sites and built structures in as much as they are or may be affected by the state of the elements of the environment referred to in (a) or, through those elements, by any of the matters referred to in (b) and (c).

Requests for information under FOI and EIR

Any requests received should be forwarded to the SPOC, who will log the request and acknowledge it within five school days.

The SPOC is responsible for:

- Deciding whether the requested information is held
- Locating, retrieving or extracting the information
- Considering whether any exemption or exception might apply and the balance of the public interest test and/or adverse effect test
- Preparing the material for disclosure and drafting the response
- Seeking any necessary approval for the response
- Sending the response to the requester.

FOI requests must be made in writing. We will only consider requests that provide a valid name and address and will not consider requests that ask us to click on electronic links. EIR requests can be made verbally; however, we will endeavour to follow up in writing with the requestor to ensure accuracy.

The SIRO and SPOC will jointly consider all requests where a public interest test is applied or where there is any doubt on whether an exemption or exception should be applied. In applying the public interest test, they will:

- Document clearly the benefits of both disclosing or withholding the requested information
- Where necessary, seek guidance from the DPO and previous case law to decide where the balance lies.

We will adopt a model publication scheme and publish as much information as possible on our website to ensure transparency and accountability.

We will charge for supplying information at our discretion, per current regulations. If a charge applies, the applicant will receive written notice, and payment must be made before the information is supplied.

We will respond to requests within the statutory timeframes of 20 school days for FOI requests and 20 working days for EIR requests.

Internal reviews

Complaints regarding FOI and EIR will be processed as an internal review request and should be made within 40 working days of the applicant receiving the original response. After that time, we will not be obliged to respond to the request for a review.

An internal review will be handled by an appropriate member of staff who was not involved in the original request. They will examine the original request and the response sent and decide whether it was handled appropriately, according to legislative requirements. The reviewing officer will also decide whether to uphold or overturn the decision to withhold information. A full response will be provided within 20 school days.

If an individual remains dissatisfied after we have concluded our internal review, they may appeal to the Information Commissioner's Office. Its contact details are below:

The telephone helpline (0303 123 1113) is open Monday to Friday between 9 a.m. and 5 p.m. (excluding bank holidays). Alternative methods to report, enquire, register, and raise complaints are available on the ICO's website here.

Appendix 4 – Surveillance

Introduction

This document concerns our use of surveillance technology and related processing of personal data. It is written in accordance with data protection and human rights legislation, statutory guidance, and relevant codes of practice. Brighter Futures Learning Partnership Trust also has a CCTV Policy which explicitly sets out the acceptable use of CCTV across the trust.

Definition of surveillance

Surveillance is the close observation or monitoring of people's activities either by physical means, such as surveillance camera systems, or by the collection and analysis of personal data, such as monitoring emails, phone calls, and internet browsing.

We will not operate covert surveillance technologies; therefore, this policy does not cover the use of such technology.

Surveillance camera systems

A surveillance camera system, formally called CCTV, includes the cameras and all the related hardware and software for transmitting, processing, and storing the captured data. We will operate surveillance camera systems to:

- Protect our buildings and property.
- Protect the safety and wellbeing of pupils, our workforce and visitors.
- Deter and discourage anti-social behaviour such as bullying, theft, and vandalism.
- Monitor compliance with our rules, codes of conduct and policies.
- Support the police in the prevention and detection of crime.

E-monitoring

'E-monitoring' or 'digital monitoring' is when an organisation uses software to monitor a user's activity on an electronic device or network. We will deploy e-monitoring software across our network, covering fixed and portable devices (PCs, laptops, and tablets), including guest devices connected to our network.

The software will monitor typed activity and the content visible on a user's screen to detect inappropriate use. Inappropriate use will be reported to designated staff within our organisation through a screenshot and other relevant technical details for further investigation. Staff, students and guests accessing our network are subject to this monitoring.

We operate e-safety monitoring software to:

- Safeguard our pupils and staff.
- Promote wellbeing and early intervention in high-risk incidents.

- Ensure appropriate use of our assets and resources.
- Monitor compliance with our rules and policies.

Data protection by design and default
Under the UK GDPR, we must consider and address privacy implications for data subjects when implementing new data processing systems. This is known as privacy by design. The usual method for assessing privacy risks to individuals is to carry out a Data Protection Impact Assessment (DPIA).

A DPIA is mandatory for surveillance activities since they are deemed particularly privacy intrusive. We will ensure that DPIAs are completed for any surveillance system and that there are no unmitigated high risks to the rights and freedoms of data subjects. In addition, we will review and update the relevant DPIA if any substantive changes are made to our systems.

We are open and transparent about using surveillance technology and identify whether we are a controller or joint controller of the information. Where we use external providers to process the data on our behalf, we will have a written contract meeting the requirements of Article 28 of the UK GDPR. We will only use providers who can ensure they have appropriate measures to safeguard the data.

Transparency
The use of surveillance camera systems must be visibly signed. Signage will include the purpose of the system, the name of the organisation operating the system and details of who to contact about its use. The signage will be clear and unobstructed so that anyone entering the area knows they are being recorded.

Users will be informed of e-monitoring in relevant policies, newsletters, internal communications, and visual cues such as notifications on computer log-in screens and/or on the browser page when they join the network.

We will ensure we are transparent about call recording by including an automatic message for inbound calls that plays before the call connects and states that calls will be recorded. We will add information about call recording to our website on the Contact Us web page and include it in new pupil and employee starter packs.

Our privacy notices will include more detailed information about our use of surveillance technologies, including information about data subject rights.

Access controls
Surveillance system data will only be accessed to comply with the specified purpose. For example, footage of camera systems intended to prevent and detect crime will only be examined where evidence suggests criminal activity has occurred. Logs of e-monitoring systems intended to safeguard children will only be examined where there

is reasonable cause to believe a child is at risk. Call recordings will be only accessed if it is deemed necessary to meet one of the purposes described above.

Each system will have proportionate access controls and a nominated Information Asset Owner (IAO) who will be responsible for its governance and security. The IAO may authorise other specified staff members to access data on the systems routinely or on an ad-hoc basis.

Ad-hoc requests and disclosures
An individual's request for surveillance data held about them will be treated as a subject access request (SAR). See Appendix Two.

Requests for surveillance data from an official agency, such as the police or insurance providers, will be processed as ad hoc disclosure requests. We will confirm the purpose of the request and the lawful basis for accessing the data. We may also require formal documentation in support of the request. If we have any concerns about such requests, we will liaise with our Data Protection Officer (DPO).

All requests for surveillance data will be recorded on a log detailing who made the request, the purpose, whether the information was disclosed or refused, and the authorising staff member.

Records of processing and retention
Under Article 30 of the UK GDPR, we have a duty to ensure that all our data processing activities are recorded for accountability purposes. To fulfil this requirement, we maintain an Information Asset Register and ensure that the use of surveillance systems is detailed on it. Any external providers processing surveillance data on our behalf are included in our data processor register.

Surveillance records will only be held as long as necessary to fulfil the specific purpose and will be deleted in accordance with our retention schedule.

Reviews
Surveillance systems must be reviewed annually to ensure they remain necessary, proportionate and effective. We will update the DPIAs to reflect any changes in system use or data collection type. The relevant IAO is responsible for ensuring reviews are completed, and evidence of this is maintained.

We will use the checklist included in Appendix A of this document to review our surveillance camera systems.

Appendix A – Surveillance Camera System Checklist

School or Trust name:		
Name and description of surveillance system:		
The system addresses the purpose and requirements (i.e., the cameras record the required information).	**YES**	**NO**
	Notes:	
The system is fit for purpose and produces clear images of adequate resolution.	**YES**	**NO**
	Notes:	
Cameras are sited in effective positions to fulfil their task.	**YES**	**NO**
	Notes:	
Cameras are positioned to avoid capturing images of persons not visiting the premises and/or neighbouring properties.	**YES**	**NO**
	Notes:	
Visible signs show that cameras are in operation. These signs include: ▪ Who operates the system; ▪ Their contact details; ▪ The purpose of the system.	**YES**	**NO**
	Notes:	
Camera recordings are securely stored, and access is limited.	**YES**	**NO**
	Notes:	

The system has the capability to fulfil a request for an individual's own personal information or an ad-hoc disclosure.	**YES**	**NO**
	Notes:	
The system has a set retention period, and records outside of retention are deleted.	**YES**	**NO**
	Notes:	
Authorised users can selectively delete information inside the retention period to fulfil the right to erasure.	**YES**	**NO**
	Notes:	
All operators have been authorised by the IAO and have completed mandatory data protection training.	**YES**	**NO**
	Notes:	
The system has been added to the IAR and data processing register.	**YES**	**NO**
	Notes:	

Checklist completed by: Name: Job title: Date:

Appendix 5 – Biometrics

Introduction

This document sets out how we collect and process biometric data. The nature of this processing, including what information is processed and for what purpose, is outlined in our privacy notices and Appropriate Policy Document.

We will comply with the additional requirements of sections 26 to 28 of the Protection of Freedoms Act 2012. These provisions relate to the use of biometric data in schools and colleges that use an automated biometric recognition system. These provisions are in addition to the requirements of data protection legislation.

Definition of biometric data

Biometric data is personal data relating to an individual's physical, physiological, or behavioural characteristics that allow identification. This can include fingerprints, facial shapes, retina and iris patterns, hand measurements, and biological or behavioural characteristics (e.g., information about a person's voice, walk, or handwriting).

An automated biometric recognition system uses technology 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 a system to determine if a match exists, allowing for recognition or identification of the individual. For example, where a fingerprint or facial recognition is used to identify an individual and allow them access to an account.

Biometric data that can identify an individual is defined in the UK GDPR and the Data Protection Act 2018 as a special category of personal data, and therefore requires additional security measures to process it.

Definition of processing

Processing of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data, including, but not limited to, disclosing, deleting, organising, or altering it. An automated biometric recognition system processes data when:

a) Recording pupil or staff biometric data, for example, by taking measurements from a fingerprint or face via a scanner.
b) Storing pupil or staff biometric information on a database system.
c) Using that data as part of an electronic process, for example, by comparing it with biometric information stored in a database to identify or recognise pupils or staff.

We process the following biometric data:

- Fingerprints – for making cashless payments, and/or accessing electronic devices

Biometric data must only be processed where there is a lawful basis, as defined in data protection legislation.

Lawful basis – explicit consent
As per guidance from the Department for Education (Protection of Biometric Data of Children in Schools and Colleges 2022), where a pupil is under 18, consent for the processing of biometric data must be sought from the pupil's parents or guardians. Explicit consent for processing the biometric data of other individuals (such as staff) will be sought directly.

We will ensure that members of staff, the pupil, and both their parents or guardians (where possible) are informed of our intention to process the individual's biometric data. This will be carried out through readily available privacy notices and communications before or at the point of obtaining consent and will include:

- The type of biometric data
- What it will be used for
- The individual's right to withdraw or refuse consent
- What the alternative arrangement will be if consent is refused or withdrawn

Under no circumstances will we collect or process a pupil's biometric data without their explicit consent or the consent of at least one authorised parent or guardian. If one parent objects in writing, we will not process that child's biometric data.

We will ensure that consent is clear, specific, and transparent and can be withdrawn at any time in accordance with the UK GDPR. We will regularly review consents to ensure that the relationship, processing, and purposes have not changed.

If a student under 18 objects to the processing of their biometric data, this will override the consent of the parents or guardians, and processing will not continue under any circumstances.

We will ensure that alternative solutions are presented to staff, pupils, and parents when consent is sought, allowing individuals to provide or refuse consent freely. Any alternative solution that is provided will not disadvantage the individual.

Data protection by design and default
We will adopt a data protection by design and default approach to processing biometric data. We will consider data protection and privacy risks from the outset and throughout the processing period.

When a new system involving biometric data or a new form of biometric data processing is introduced, we will ensure that a DPIA is completed before implementing the project. This addresses any associated risks and considers the potential impact the processing may have on pupils, staff, and the wider community.

We will be open and transparent about using biometrics and identify whether we are a controller or joint controller of the information. When we use external providers to process data on our behalf, we will have a written contract that meets the requirements of Article 28 of the UK GDPR. We will only use providers who can ensure they have appropriate measures to safeguard the data.

Bias and/or discrimination

We understand that there may be bias or discrimination when using systems which utilise biometric data. To mitigate any risk resulting from bias and discrimination, we will:

- Ensure that systems have been trained using a sufficient volume and variety of data, use bias-mitigation techniques, and implement fairness metrics.
- Be open and transparent about any known biases.
- Integrate human oversight to review and validate outputs.

We will only process biometric data where we have deemed it necessary and proportionate. We will also consider whether we need to complete an Equalities Impact Assessment to fulfil our obligations under the Equalities Act 2010.

Retention and destruction

Biometric data will be encrypted and stored securely to prevent unauthorised or unlawful use. It will only be used for the purpose for which it was obtained. Our security measures will be regularly tested to ensure they remain effective.

Biometric data will be securely destroyed when consent is withdrawn or when processing is no longer required for its intended purpose, for example, when the pupil no longer uses the system or has left the school.