Data Protection Policy

Document History	
Created or reviewed:	Autumn 2023
Reviewing officer:	Headteacher/SLT
Review frequency:	2 yearly
Review date:	Autumn 2025

Version Control			
Version	Date	Notes and amendments	Approval
0.1	13/09/2023	Initial draft	GB
0.2	14/09/2023	Edits following feedback from Headteacher	
1.0	14/09/2023	Published Copy	

Contents

INTRODUCTION AND SCOPE 3

ROLES AND RESPONSIBILITIES 3

DATA PROTECTION PRINCIPLES 4

LAWFUL BASES 5

CONSENT 5

DATA SUBJECT RIGHTS 5

RECORDS OF PROCESSING 6

PRIVACY BY DESIGN AND RISK ASSESSMENTS 6

INFORMATION SHARING 6

CONTRACT MANAGEMENT 7

TRAINING 7

COMPLAINTS 7

APPENDIX ONE – APPROPRIATE POLICY DOCUMENT (APD) 9

APPENDIX TWO – SUBJECT ACCESS REQUEST (SAR) PROCEDURE 12

APPENDIX THREE – FREEDOM OF INFORMATION (FOI) AND ENVIRONMENTAL INFORMATION REGULATION (EIR) REQUESTS 13

Introduction and Scope

Brooklands School 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.

Commented [KR1]: Please note that if you are a part of a MAT this should be the Trust name

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), Environmental Information Regulations 2004 (EIR) and Freedom of Information Act 2000 (FOIA), as well as associated guidance and Codes of Practice issued under the legislation.

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 behalf of, the school. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

This policy is the school's main information governance policy and applies to all personal data, regardless of whether it is in paper or electronic format.

Information security, data breaches, acceptable use of systems and records management are addressed in separate policies.

Roles and Responsibilities

Overall responsibility for ensuring that the school meets the statutory requirements of any data protection legislation lies with the Board of Governors or Trustees. The following roles have day to day responsibility for compliance and provide the necessary assurance to the Board.

Data Protection Officer (DPO)
The role of the DPO is to assist the school in monitoring compliance with the UK GDPR and the Data Protection Act 2018 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 UK GDPR and other data protection laws,
- Monitoring compliance with data protection legislation and internal policies,

- Raising awareness of data protection issues and conducting compliance reviews, and
- Liaising with the Information Commissioners Office (ICO).

Senior Information Risk Owner (SIRO)
The SIRO is a senior member of staff who has ultimate responsibility for operational risk, ensuring that the school's policies and procedures are effective and comply with legislation, and promoting good practice in school. In our organisation this role lies with the Headteacher.

Single Point of Contact (SPOC)
The SPOC is someone at school level who can take operational responsibility for data protection, including communicating with data subjects and the DPO. In our organisation this role lies with the School Business Manager.

Information Asset Owner (IAO)
An IAO is an individual who is responsible for the security and maintenance of a particular information asset. They are responsible for ensuring that other members of staff are using the information safely and responsibly. We will ensure that IAO's are appointed based on sufficient seniority and level of responsibility, and document this 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 behalf of, the school are responsible for collecting, storing and processing any personal data in accordance with this policy.

Data Protection Principles

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

- Processed lawfully, fairly and in a transparent manner **(Lawfulness, Fairness and Transparency**).
- Collected only for specified, explicit and legitimate purposes (**Purpose Limitation**).
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (**Data Minimisation**).
- Accurate and where necessary kept up to date (**Accuracy**).
- Not kept in a form which 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 against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**).

We recognise that not only must we comply with the above principles, we must also demonstrate our compliance **(Accountability).**

Lawful Bases

UK GDPR sets out several conditions under which we can process personal information lawfully. We usually rely on the lawful basis of Public Task or Legal Obligation, however at times we may rely on our legitimate interests. We will only do this where we are using data in ways individuals would reasonably expect and will carry out an appropriate legitimate interest assessment (LIA) prior to starting the processing.

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

Consent

We generally only obtain consent where there is no other lawful basis, for example when taking photographs or videos intended for publication. We will ensure that consent is clear and transparent and can be withdrawn at any time, in accordance with the UK GDPR. We will regularly review consents to check that the relationship, the processing, and the purposes have not changed.

Where appropriate we will seek consent directly from pupils over the age of 12 years. Where this is not appropriate, or pupils are under the age of 12 years, we will seek consent from the parent or guardian.

Commented [SA2]: Check that this is accurate for your school. Some settings may differ.

Data Subject Rights

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

Right to be informed
We provide individuals with privacy information at the time we collect their data, normally by means of a privacy notice, which is 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 have in place a SAR procedure which 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 member of staff, but we encourage requests to be made in writing, wherever possible, and forwarded to 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 in respect of the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision made.

Records of Processing

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

- The school or Trust'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 bases for each processing activity,
- The format and location of the personal data,
- Details of any transfers to third countries, and the appropriate safeguards,
- The retention periods for each asset,
- A general description of the technical and organisational security measures.

We will include links to relevant documentation, such as data processing contracts, information sharing agreements, and risk assessments, wherever possible.

We will 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 a privacy by design approach and implement appropriate technical and organisational security measures to demonstrate how we 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 purpose of the DPIA is to consider and document the risks associated with a project prior to its implementation, ensuring data protection is embedded by design and default.

All of the data protection principles will be assessed to identify specific risks. These risks will be evaluated and solutions to mitigate or eliminate these risks 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.

All DPIAs are signed by our Senior Information Risk Owner and Data Protection Officer.

Information Sharing

In order to efficiently fulfil our duty of education provision it is sometimes necessary for us to share information with third parties. Routine and regular information sharing arrangements will be documented in our privacy notices and in our IAR.

Any further or ad-hoc sharing of information will only be done so 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 to do so, 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 contractors 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 there is a written contract in place which includes all the mandatory data processing clauses, as required by 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.

International Transfers

Usually, personal information processed by us is not transferred outside of the European Economic Area (EEA), which is deemed to have adequate data protection standards by the UK government. If personal data is transferred outside the EEA, we will take reasonable steps to ensure appropriate safeguards are in place.

We will consult with the DPO for any processing which may take place outside of the EEA prior to any contracts being agreed.

Training

We will ensure that appropriate guidance and training is given to our workforce, governors or Trustees, and other authorised school users on data protection and access to information. Training will be delivered as part of the induction process and as refresher training at appropriate intervals.

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

Complaints

We take complaints seriously, and any concerns about the way we have handled personal data or requests for further information in relation to data protection, should be raised with SPOC. We will then liaise with the DPO, where necessary, for advice and guidance.

If an individual remains dissatisfied after we have concluded our investigation, they may complain to the Information Commissioner's Office. Their contact details are below:

Phone: 0303 123 1113 or via their live chat. Their normal opening hours are Monday to Friday between 9am and 5pm (excluding bank holidays). You can also report, enquire, register and raise complaints with the ICO using their web form on Contact us | ICO.

Appendix One - Appropriate Policy Document (APD)

Introduction

Brooklands School processes special category and criminal conviction data in the course of fulfilling its functions as a school. Schedule 1 of the Data Protection Act 2018 requires data controllers to have in place an 'appropriate policy document' where certain processing conditions apply for the processing of special categories of personal data and criminal convictions data. This policy fulfils this requirement.

This policy complements our existing records of processing as required by Article 30 of UK General Data Protection Regulation, which has been fulfilled by the creation and maintenance of an Information Asset Register. It also reinforces our existing retention and security policies, procedures and other documentation in relation to special category data.

Special categories and conditions of processing

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

- racial or ethnic origin,
- religious or philosophical beliefs,
- trade union membership,
- health,
- sex life/orientation,

We also process criminal offence (CO) data under Article 10 of UK GDPR, including for pre-employment checks and declarations by employees in line with their contractual obligations.

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

Article 9(2)(a) – explicit consent
We make sure that consent given by any person is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing. We regularly review consents to ensure they remain up to date.

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

Examples include when we carry out DBS checks on staff to evidence suitability for a role; collect medical information to put in reasonable adjustments at work and monitor staff absence; and keep 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 rely on for this processing is **Schedule 1, Part 1, (1) - employment, social security and social protection.**

Article 9(2)(g) – reasons of substantial public interest
We have a wide variety of duties we must carry out in the public interest. Much of our processing of SC data is done so for the purposes of substantial public interest.

Examples include when we process SC data to identify students who require additional support such as special educational needs; processing safeguarding concerns to ensure the safety and wellbeing of pupils; or collecting medical information when monitoring pupil attendance 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 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 have several policies and procedures in place to ensure our compliance with the Article 5 Data Protection Principles and meet our accountability obligations, explained in more detail below:

Accountability principle
We have put in place appropriate technical and organisational security measures to meet the requirements of accountability. These include:

- The appointment of a Data Protection Officer, Veritau, which provides reports to the Board of Governors.
- Taking a data protection by design and default approach to our processing activities, including the use of risk assessments.
- Maintaining documentation of our processing activities through an Information Asset Register.
- Adopting and implementing information governance policies and ensuring we have written contracts in place with data processors.
- Implementing appropriate security measures in relation to the personal data we process. More detail can be found in our Information Security Policy.

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

We consider how any 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 policy document. All privacy notices provide details of data subject rights. Our privacy information is regularly reviewed and updated to ensure it accurately reflects our processing.

Principle (b): purpose limitation
Schools can only act in ways and for purposes 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 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 check that it is compatible with our original purpose, or we obtain specific consent for the new purpose.

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

Principle (d): accuracy
Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is processed, we will take every reasonable step to ensure that data is erased or rectified without delay. Where we are unable to 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 all reasonable steps to inform them of the inaccuracies and rectification. We maintain a log of all data rights requests and have appropriate processes for handling such requests.

Principle (e): storage limitation
We have a Retention Schedule in place which is based on guidance issued by the Information and Records Management Society (IRMS). Where there is no legislative or best practice guidance in place, the SIRO will decide how long the information should be retained based on the necessity to keep the information for a legitimate purpose or purposes. We also maintain a Destruction Log, which documents what information has been destroyed, the date it was destroyed and why it has been destroyed. Further information can be found in our Records Management Policy.

Commented [SA3]: Remove if your retention schedule is not based on the IRMS toolkit.

Principle (f): integrity and confidentiality (security)
We 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 in a log, investigated, and reported to our Data Protection Officer where necessary. High risk incidents are reported to the Information Commissioner's Office. This process is documented in greater detail in our Information Security Policy.

Retention of special category and criminal convictions data

The retention periods of special category and criminal convictions data are set out in our Retention Schedule. Retention periods of specific information assets are identified in our Information Asset Register and we have in place a Records Management Policy.

Appendix Two - Subject Access Request (SAR) Procedure

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

Commented [KR4]: This is our suggested time frame for acknowledgement, but you may specify a different time frame if you prefer

We must be satisfied of 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, or
- 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.

We can apply a discretionary extension of up to a further two calendar months to comply if the requested information would take a considerable amount of time to respond, due to either the complexity or volume of the records. If we wish to apply an extension, we will firstly seek guidance from our DPO, then inform the applicant of the extension within the first calendar month of receiving the request.

If we think it necessary to apply any exemptions, we will seek guidance from our DPO. In limited circumstances, we may also refuse a request on the basis that it is manifestly unreasonable or excessive.

For maintained and special schools only:
Requests received from parents asking for information falling under the pupil's education record will be dealt with under the Education (Pupil Information) (England) Regulations 2005 and responded to within 15 school days. Any charges which arise from this request will be applied at our discretion.

Commented [SA5]: Please delete depending on your setting.

Internal Review

Complaints in relation to SARs and other data subject rights will be processed as an internal review request.

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

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

Phone: 0303 123 1113 or via their live chat. Their normal opening hours are Monday to Friday between 9am and 5pm (excluding bank holidays). You can also report, enquire, register and raise complaints with the ICO using their web form on Contact us | ICO.

Appendix Three – 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. Schools 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 general 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 the handling of requests for information. To comply with this Code requests must:

- Be in writing,
- Provide the name or company name and contact address or email address,
- Describe the information they are requesting,
- 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 a 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 that relates to the environment, including activities which may affect the environment, are dealt with under the Environmental Information Regulations 2004. EIR is similar to FOI but there is an even greater presumption of disclosure, and there are 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 address or email address,
- A description of the information being requested,
- Ideally, 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), and

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 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,
- Preparing the material for disclosure and drafting the response,
- Seeking any necessary approval for the response, and
- Sending the response to the requester.

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

The Chair of Governors and Headteacher will jointly consider all requests where a public interest test is applied or where there is any doubt on whether an exemption 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 previous case law in deciding where the balance lies,

- Consult the DPO.

Reasons for disclosing or not disclosing will be reported to the next governing board or committee meeting.

We have adopted the Information Commissioner's model publication scheme for schools and will publish as much information as possible on our website in the interests of transparency and accountability.

We may charge for supplying information at our discretion, in line with current regulations. If a charge applies, written notice will be given to the applicant and payment must be received before the information is supplied. We will follow our Local Authority's charging regime for FOI/EIR.

We will adhere to the required FOI and EIR timescales, and requests will be responded to within 20 school days.

Internal Reviews

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

An internal review will be dealt with by an appropriate member of staff who did not have any involvement in the original request. They will examine the original request and the response that was sent and decide whether it was dealt with appropriately, according to legislative requirements. The reviewing officer will also decide whether to uphold or overturn the decisions 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. Their contact details are below:

Phone: 0303 123 1113 or via their live chat. Their normal opening hours are Monday to Friday between 9am and 5pm (excluding bank holidays). You can also report, enquire, register and raise complaints with the ICO using their web form on Contact us | ICO.

Copyright

We will take reasonable steps to inform enquirers if any third party might have a copyright or intellectual property interest in information provided in response to their requests. However, it will be the enquirer's responsibility to ensure that any information provided by us is not re-used in a way which infringes those interests, whether or not any such warning has been given.

Appendix x - Surveillance Policy

Commented [KR6]: You must include this appendix if you use CCTV, e-monitoring or call recording.

Please remove any sections not applicable.

Introduction

This policy concerns our use of surveillance technology and related processing of personal data. It is written in accordance with data protection and human rights legislation and relevant codes of practice.

Surveillance is the close observation or monitoring of individuals or spaces, for the purpose of influencing behaviour or protecting people. We do not operate covert surveillance technologies and therefore this policy does not cover the use of such technology.

Commented [AJ7]: Please note that this policy only covers use of CCTV cameras, e-monitoring software and call recording. If your school carries out any other forms of surveillance, such as body-worn cameras, please contact us to find out how you need to adapt this policy.

Commented [KR8]: Please ensure you are not monitoring individuals or spaces covertly, i.e., without informing people about it.

We operate e-safety monitoring software systems to:

- Safeguard our pupils and staff
- Promote wellbeing and early intervention
- Ensure appropriate use of school assets and resources
- Monitor compliance with school rules and policies

Commented [KR9]: We have identified the most likely purposes for using e-monitoring but please add any specific purposes that are not covered.

The school uses Smoothwall

Privacy Risk Assessment

Under the UK GDPR, we are required to consider and address privacy implications to 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 by carrying out a Data Protection Impact Assessment (DPIA).

A DPIA is mandatory for surveillance activities since they are deemed particularly intrusive. We will ensure that DPIAs have been completed e-monitoring 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 we substantively change our systems.

Commented [KR10]: Please ensure that you have completed DPIAs using the Veritau templates, and this statement reflects the outcome.

We will ensure we have completed the Privacy by Design checklist for call recording.

Contract Management

We are required to have contracts with any data processors we use, containing certain data processing clauses prescribed by law. We will ensure that we have implemented an appropriate contract with the e-monitoring systems to allow for them storing, monitoring or accessing the data on our behalf. We will only agree to these contracts where they have been assessed for compliance and determined to meet our requirements.

Commented [KR11]: If you have more complicated arrangements which include other third parties, please let us know and we can advise on alternative wording for this section.

Commented [KR12]: Please ensure you have a data processing contract in place with each provider, it has been checked for the mandatory clauses and you are comfortable with the level of compliance.

Transparency

The use of CCTV 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 the system. The signage will be clear and kept unobstructed, so that anyone entering the area will be aware that they are being recorded.

Commented [KR13]: Remove if you do not use CCTV

The use of e-monitoring systems must also be clearly signed. Users will be made aware of the e-monitoring by a notice on the log in screen of computers and/or on the browser page when they join the network.

Commented [KR14]: These are common methods of informing users but please liaise with your IT team or software provider and amend our wording to reflect how users will be informed of the monitoring.

Commented [KR15]: Remove if you do not use e-monitoring

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 information in new children and employee starter packs.

More detailed information about use of CCTV and e-monitoring must also be provided via a Privacy Notice, which must also inform data subjects about their rights in relation to their surveillance data. We have included the mandatory privacy information to data subjects in our relevant privacy notices.

Access Controls

Surveillance system data will only be accessed to comply with the specified purpose. 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.

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

Disclosures

A request by an individual for surveillance data held about them will be treated as a subject access request (SAR). For more information on data subjects' right of access to their information, please refer to our Data Protection Policy.

If we receive a request for surveillance data from an official agency, such as the police, then we will confirm the purpose of the request and their lawful basis for accessing the data. We may also require formal documentation in support of the request. We will liaise with our Data Protection Officer (DPO) if we have any concerns about such requests.

Record of Processing and Retention

We have a duty under Article 30 of the UK GDPR to ensure that all our data processing activities are recorded for accountability purposes. We maintain an Information Asset Register to fulfil this requirement. We will ensure that the use of surveillance systems is detailed on this register.

Surveillance records will only be held as long as necessary to fulfil the specific purpose and deleted in line with our Records Management Policy.

Reviews

CCTV systems must be reviewed annually to ensure that systems still comply with data protection legislation and national standards. The IAO should use the checklist included in Appendix A of this policy to complete this review.

The school should review the e-monitoring systems regularly by undertaking a review of the DPIA and updating the DPIA to reflect any changes in how the system is used or the type of data that is collected.

Commented [AJ16]: Remove if you do not record telephone calls.

Commented [KR17]: Please ensure you have these measures in place so that this statement is accurate.

Commented [KR18]: Remove if you do not use e-monitoring

The school should review the call recording systems regularly by undertaking a review of the Privacy by Design checklist and updating it to reflect any changes in how the system is used.

It is the responsibility of the relevant IAO to ensure reviews are completed and evidence of this is maintained.

Complaints

Complaints by individuals about the use of surveillance systems or data will be treated as a data protection concern. For more information on data protection complaints, refer to our main Data Protection Policy.