Data Protection Policy

Applicable to:	✓	All individual schools within NEAT Academy Trust
	×	Specified schools only within NEAT Academy Trust
	✓	Central Team within NEAT Academy Trust
	✓	NEAT Active Ltd
Approval body:	NEAT Academy Trust Finance, Audit and Risk Committee, which may be delegated NEAT Active Ltd Board of Directors, which may be delegated	

Statutory policy	No
Statutory requirement to publish on website	No
If not, agreed to publish on website?	Yes – trust, school and Benfield Sports Centre

Review Date	
Frequency	**Next Review Due**
Every 3 years	December 2026 (or earlier if new guidance or legislation issued and/or business need for earlier review identified)

Version Control:

Author	Date	Version	Status	Notes
Central Support Manager (SH)	24/05/18	1.0	Final	Approved version for implementation.
Director of HR and Governance (SH)	10/04/19	2.0	Final	Very minor corrections.
Governance Support Manager (HH)	11/12/20	3.0	Final	Amended to reflect updated guidance from ICO about charging for SARs.
Governance Support Adviser (HH)/Head of Governance and Corporate Affairs (SH)	26/03/21	4.0	Final	Amended to become joint policy for NEAT Academy Trust and NEAT Active Ltd to apply from 01.04.21 and to include special category data.
Head of Governance and Corporate Affairs (SH)	12/04/21	5.0	Final	Very minor amendments to DPO contact details.
Head of IT Services (ABux)	05/12/23 FAR Comm 15/12/23 NAL Board	6.0	Final	Amended version to align to revised Veritau model policy.

Contents

1 Purpose

The purpose of this policy is to set out how we protect the personal data that we collect, store and process in relation to key stakeholders and how we deal with requests in relation to that data.

2 Scope

This policy applies to both NEAT Academy Trust and its subsidiary company, NEAT Active Ltd, (the NEAT Group).

Each organisation is a data controller and is required to process personal data about pupils, parents/carers, employees, job applicants, members, non-executive directors/trustees, local governing committee members, volunteers, service users/customers and other individuals we interact with in accordance with data protection and other relevant legislation.

This policy applies to our employees, non-executive directors, local governing committee members, contractors, agents and representatives, volunteers and agency workers working for, or on behalf of, the organisation.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Information security (including data breaches), acceptable use of systems and records management are addressed in separate NEAT Group policies and agreements.

Each organisation also has its own separate Freedom of Information Policy and Information Publication Scheme.

3 Policy statement – data protection principles

We will ensure that personal data is processed in accordance with the requirements of data protection legislation and that we comply with the principles specified in the legislation that data will be:

- processed lawfully, fairly and in a transparent manner in relation to individuals **(Lawfulness, Fairness and Transparency**);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**Purpose Limitation**);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**Data Minimisation**);
- accurate and, where necessary, kept up-to-date (**Accuracy**);
- 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 (**Storage Limitation**); and
- 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 (**Security, Integrity and Confidentiality**).

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

4 Legal considerations

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
- associated guidance and Codes of Practice issued under the legislation.

5 Roles and responsibilities

- **NEAT Academy Trust and NEAT Active Ltd Boards of Directors:** have overall responsibility for ensuring that the organisations meet the statutory requirements of any data protection legislation. The Finance, Audit and Risk Committee provides scrutiny and evaluation of the trust's responsibilities for information governance on behalf of the Board. Day-to-day responsibility for compliance and providing the necessary assurance is delegated to the following roles by the Boards.

- **Data Protection Officer (DPO):** assists the organisations in monitoring compliance with the UK GDPR and the Data Protection Act 2018 and advises on data protection issues.

  We have appointed Veritau as our DPO. Veritau's contact details are follows:

  Schools Data Protection Officer
  Veritau
  West Offices
  Station Rise
  York
  YO1 6GA
  schoolsDPO@veritau.co.uk// 01904 554025

  The DPO is an advisory role, and duties include:
  - informing and advising us and our workforce and governance volunteers 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 Commissioner's Office (ICO).

- **Senior Information Risk Owner (SIRO):** The SIRO is a senior member of staff who has ultimate responsibility for operational risk, ensuring that our policies and procedures are effective and comply with legislation, and promoting good practice. In our organisations this role lies with NEAT Academy Trust's Head of Business Services.

- **Single Point of Contact (SPOC):** The SPOC is someone at local level who can take operational responsibility for data protection, including communicating with data subjects and liaising with the trust's Data and Information Governance Manager. In schools, this is a member of our Business Support Team: Operations Manager, Business Support Manager or Senior Administrator; in the NEAT Central Team, this is the Data and Information Governance Manager; for

NEAT Active Ltd, this is the Sports Centre Manager; for Newcastle PE and School Sport Service (NPESSS), this is PE and School Sport Assistant 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 IAOs are appointed based on sufficient seniority and level of responsibility, and document this in our Information Asset Register (IAR).

- **Data and Information Governance Manager (DIGM):** The DIGM provides advice and guidance about all data protection matters, liaises with the DPO/ICO and provides co-ordination and oversight of subject access requests.

- **Stakeholders:** Everyone working for, or on behalf of, the organisations including employees, non-executive directors, local governing committee members, contractors, agents and representatives, volunteers and agency workers, is responsible for collecting, storing and processing any personal data in accordance with this policy. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary or other action.

6 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 (Appendix 1) 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.

7 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/carer or guardian.

8 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 2).

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, via email to the Data and Information Governance Manager at information.governance@neatat.org.uk, 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.

9 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 organisation/school'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; and
- 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.

10 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.

11 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.

12 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.

13 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.

14 Training

We will ensure that appropriate guidance and training is given to our workforce, governance volunteers and other authorised 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.

15 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 will be processed as an internal review request. We will then liaise with our DPO, where necessary, for advice and guidance.

An internal review should be requested by email to:
information.governance@neatat.org.uk
or in writing to:
NEAT Academy Trust, Hedley Court, Orion Business Park, North Shields, Tyne and Wear NE29 7ST

We will liaise with our DPO, where necessary, for advice and guidance.

An internal review will be dealt with by an appropriate member of staff who did not have any involvement in the original matter. They will examine how the matter was handled and the initial response 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 one calendar month where possible.

There may be circumstances where we require more time to complete an internal review, for example if we need to address complex issues, consult with third parties or consider substantial amounts of information. In these circumstances we will inform the requestor that we will need more time and provide a reasonable target date. This will usually be no more than an additional calendar month, unless there are legitimate reasons why a longer extension is necessary.

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.

General

This policy is at the discretion of the boards of directors and can be varied at any time. In the event of any conflict with primary legislation or statutory regulations, the legal provisions will have precedence over this policy in all cases.

Appendix 1 – Appropriate Policy Document (APD)

Introduction

The organisations process special category and criminal conviction data in the course of fulfilling their functions. 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 of data:

- racial or ethnic origin;
- religious or philosophical beliefs;
- trade union membership;
- health;
- sex life/orientation;
- biometric identifiers (only applicable at the following: Benfield School, St Hild's Church of England School and Walkergate Community School).

We also process criminal offence data under Article 10 of UK GDPR, including for pre-employment checks and declarations by employees in line with their contractual obligations and pre-appointment checks for governance volunteers in line with regulatory requirements.

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.

  Examples of such processing include when we use biometric (fingerprint) data for identification or authentication purposes for school meal payments; when we collect diversity and analyse data to help us understand how representative our workforce and governance volunteers are of our pupil populations/local communities; or when we ask for health or medical information from visitors to aid them in the event of an emergency.

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

  Examples include when we carry out DBS checks on staff and governance volunteers 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 special category data is done so for the purposes of substantial public interest.

  Examples include when we process special category data to identify pupils 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 Boards of Directors.
  - 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 special category or criminal offence 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**
  Organisations 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**
  When 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 within our Records Management and Retention Policy, 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 and Retention Policy.

- **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

We have a Records Management and Retention Policy in place. The retention periods of special category and criminal convictions data are included in the Retention Schedule. Retention periods of specific information assets are identified in our Information Asset Registers.

Appendix 2 - 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, governors, directors, contractors or agents 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 the Data and Information Governance Manager who will log the request and acknowledge it within five school days.

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 for 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 secondary school settings/NEAT Active Ltd. only:
If a subject access request is made by a parent/carer or guardian whose child is 12 years of age or over, we may consult with the child or ask that they submit the request on their own behalf or confirm permission for the request. This decision will be made based on the capacity of the pupil in question.

Complaints

Complaints by individuals in relation to SARs and other data subject rights will be treated as a data protection concern and handled using the procedure in section 15.

Appendix 3 – Surveillance/CCTV/E-monitoring software and Call Recordings Policy

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 only use surveillance in the context of CCTV, e-monitoring software and call recording. We do not operate covert surveillance technologies and therefore this policy does not cover the use of such technology.

CCTV

We operate Closed Circuit Television (CCTV) 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 and policies; and
- support the police in the prevention, detection, investigation and prosecution of any crimes.

Each location uses different CCTV systems - please see table below.

E-monitoring and filtering software

We operate e-safety monitoring and filtering software systems to:

- safeguard our pupils, staff and governance volunteers;
- promote wellbeing and early intervention;
- ensure appropriate use of our assets and resources; and
- monitor compliance with our rules and policies.

We use Lightspeed as our monitoring and filtering software.

Call recording system

We record incoming and outgoing telephone calls at specified locations in the table below:

- for quality monitoring and staff training purposes;
- for efficient resolution of disputes and complaints;
- to assist with informal and formal investigations, where appropriate; and
- as evidence of safeguarding concerns.

Each location uses different telephone systems **-** please see table below.

Location	CCTV	Filtering and monitoring system	Call recording system
Benfield School	Vista	Lightspeed	Mitel 3300
Central Walker Church of England Primary School	Pelco DX4800	Lightspeed	Mitel 3300
NEAT Active Ltd. at Benfield Sports Centre	Vista	Lightspeed	Mitel 3300
NEAT Central Office	Through third party provider	Lightspeed	Ring Central - Yes
St Hild's Church of England School	Truvision DVR 15HD	Lightspeed	Avaya System - No
Tyneview Primary School	Ahua	Lightspeed	Mitel 3300
Walkergate Community School	GPS	Lightspeed	Mitel 3300
West Walker Primary School	Hik Vision and Viola	Lightspeed	Mitel 3300

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 for both CCTV and 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.

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 providers of our CCTV, and e-monitoring to allow for them to access 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.

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.

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 login screen of computers 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 information in packs for new pupils, employees and governance volunteers.

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. For example, footage of CCTV systems intended to prevent and detect crime will only be examined where there is evidence to suggest criminal activity has taken place. 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, see Appendix 2 Subject Access Request Procedure.

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 and Retention Policy.

Reviews

CCTV systems must be reviewed annually to ensure that systems still comply with data protection legislation and national standards. The IAO will use the checklist provided by our DPO to complete this review.

We will 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.

We will review the call recording systems regularly by undertaking a review of the Privacy by Design checklist provided by our DPO 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 and handled using the procedure in section 15.

Appendix 4 – Biometric Policy applicable to Benfield School, St Hild's Church of England School and Walkergate Community School only

Introduction

This policy 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 (see Appendix 1).

We will comply with the additional requirements of sections 26 to 28 of the Protections of Freedoms Act 2012. This includes provisions which relate to the use of biometric data in schools and colleges who use an automated biometric recognition system. These provisions are in addition to the requirements of the UK General Data Protection Regulation (UK GDPR).

Definition of Biometric Data

Biometric data is defined as personal data relating to the physical, physiological or behavioural characteristic of an individual which allows the identification of that individual. This can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

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 see if there is a match, in order to recognise or identify the individual. For example, where a fingerprint is used to identify an individual and allow them access to an account.

Biometric data is defined in the UK GDPR and the Data Protection Act 2018 as a special category of personal data, and it therefore requires additional measures to be put in place 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 pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
b) Storing pupils' biometric information on a database system; or
c) Using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database to identify or recognise pupils.

Any processing of biometric data will only be carried out where there is a lawful purpose for the processing, as defined in data protection legislation.

Consent

As per guidance from the Department for Education (Protection of biometric data of children in schools and colleges 2022), where a pupil is below the age of 18, consent for the processing of biometric data will be sought from the pupil's parents/carers or guardians.

Consent for processing of any other individual's biometric data (such as staff) will be sought directly.

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

- the type of biometric data;
- what it will be used for;
- the individual's rights to withdraw or refuse consent; and
- what the alternative arrangement will be if consent is refused or withdrawn.

Under no circumstances will we collect or process the biometric data of an individual without their explicit consent or the consent of at least one authorised parent/carer or guardian, this will be obtained prior to obtaining any biometric data. If one parent objects in writing, then we will not be permitted to take or use that child's biometric data.

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

When we collect additional biometric data or want to process the biometric data for a new purpose, new consent must be gained to ensure that the individual or their parent/carer or guardian is fully informed.

Consent can be withdrawn at any time by contacting the school office. We will ensure that, where consent is refused or withdrawn, there is an alternative solution which does not require the obtaining or processing of biometric data to ensure that any individual is not disadvantaged as a result.

If a pupil under the age of 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.

The Protection of Freedoms Act 2012 only covers processing on behalf of our organisation. If an individual is using biometric software for their own personal purposes this is classed as private use, even if the software is accessed using school or college equipment.

Security and retention

When a new system involving biometric data, or a new form of processing biometric data is introduced, we will ensure that we have completed a DPIA to address any associated risks prior to the implementation of the project.

We will ensure that we store any biometric data securely to prevent any unauthorised or unlawful use, and only use it for the purposes it was obtained. It will be securely destroyed in line with the Retention Schedule in our Records Management and Retention Policy, or when consent is withdrawn.