ANGLIAN LEARNING

Dynamic, empowered learners who thrive and lead in their communities: locally, nationally and globally

DATA PROTECTION POLICY

THIS POLICY WAS APPROVED:	AUTUMN 2021
POLICY VERSION:	2.0
THIS POLICY WILL BE REVIEWED:	AUTUMN 2024
MEMBER OF STAFF WITH RESPONSIBILITY FOR REVIEW:	DPO

SECTION I. GENERAL PROVISIONS

1. INTRODUCTION

1.1. Anglian Learning ("the Trust") collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the Trust in order provide education and associated functions. The Trust may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation and other related legislation.

1.2. The GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

1.3. Special Category Data is given special protection, and additional safeguards apply if this information is to be collected and used.

1.4. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

1.5. The information will be managed in a confidential manner. Where Covid-19 related data is to be used for general reporting or statistics, steps will be taken to anonymise the data and general numbers used, wherever possible.

1.6. The Trust does not intend to seek or hold Special Category Data (previously known as sensitive personal data) about staff or pupils except where the Trust has been notified of the information, or it comes to the Trust's attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or pupils are under no obligation to disclose to the Trust their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements).

2. DEFINITIONS

2.1. **'Personal data'** is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain[1]. A sub-set of personal data is known as 'special category personal data'. This special category data is information that reveals:

[1] For example, if asked for the number of female employees, and you only have one female employee, this would be personal data if it was possible to obtain a list of employees from the website.

2.1.1. race or ethnic origin;

2.1.2. political opinions;

2.1.3. religious or philosophical beliefs;

2.1.4. trade union membership;

2.1.5. physical or mental health (including data used for determining whether individuals have experienced or are experiencing Covid-19 symptoms or are in the high-risk categories which are more vulnerable to becoming seriously ill)

2.1.6. an individual's sex life or sexual orientation;

2.1.7. genetic or biometric data for the purpose of uniquely identifying a natural person.

2.2. **'Biometric data'**:

2.2.1. refers to personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

2.2.2. The Information Commissioner considers all biometric information to be personal data as defined by the General Data Protection Regulations and Data Protection Act.

2.2.3. The Protection of Freedoms Act 2012 includes provision which relate to the use of biometric data in schools and colleges when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the Data Protection Act.

2.3. **'Automated biometric recognition system'**:

2.3.1. Uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically).

2.3.2. An automated biometric recognition system processes data when:

1 Recording biometric data of a pupil, for example, taking measurements from a fingerprint via a fingerprint scanner;

2 Storing pupils biometric information on a database system; or

3 Using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise pupils.

2.3.3. The information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.

2.4. **'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 it, deleting it, organising it or altering it.

3. THE DATA PROTECTION PRINCIPLES

3.1. The six data protection principles as laid down in the GDPR are followed at all times:

3.1.1. personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;

3.1.2. personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;

3.1.3. personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;

3.1.4. personal data shall be accurate and, where necessary, kept up to date;

3.1.5. personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes;

3.1.6. personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3.2. In addition to this, the Trust is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in paragraphs 7 and 8 below).

3.3. The Trust is committed to complying with the principles in 3.1 at all times. This means that the Trust will:

3.3.1. inform individuals about how and why we process their personal data through the privacy notices which we issue

3.3.2. be responsible for checking the quality and accuracy of the information;

3.3.3. regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the Document Retention Policy;

3.3.4. ensure that when information is authorised for disposal it is done appropriately;

3.3.5. ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;

3.3.6. share personal information with others only when it is necessary and legally appropriate to do so;

3.3.7. set out clear procedures for responding to requests for access to personal information known as subject access requests;

3.3.8. report any breaches of the GDPR in accordance with the procedure in paragraph 9 below.

4. CONDITIONS FOR PROCESSING IN THE FIRST DATA PROTECTION PRINCIPLE

4.1. The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given.

4.2. The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.

4.3. The processing is necessary for the performance of a legal obligation to which we are subject.

4.4. The processing is necessary to protect the vital interests of the individual or another.

4.5. The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us.

4.6. The processing is necessary for a legitimate interest of the Trust or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned.

5. USE OF PERSONAL DATA BY THE TRUST

5.1. The Trust processes personal data on pupils, staff and other individuals such as visitors. In each case, the personal data must be processed in accordance with the data protection principles as outlined in paragraph 3.1 above.

6. SECURITY OF PERSONAL DATA

6.1. The Trust will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the GDPR. The Trust will take all reasonable steps

to ensure that all personal information is held securely and is not accessible to unauthorised persons.

6.2. For further details as regards security of IT systems, please refer to the ICT Policy.

7. DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES[2]

7.1. The following list includes the most usual reasons that the Trust will authorise disclosure of personal data to a third party:

7.1.1. To give a confidential reference relating to a current or former employee, volunteer or pupil;

7.1.2. for the prevention or detection of crime;

7.1.3. for the assessment of any tax or duty;

7.1.4. where it is necessary to exercise a right or obligation conferred or imposed by law upon the Trust (other than an obligation imposed by contract);

7.1.5. for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

7.1.6. for the purpose of obtaining legal advice;

7.1.7. for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);

7.1.8. to publish the results of public examinations or other achievements of the pupils of the Trust;

7.1.9. to disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips; The legal basis will vary in each case but it will usually be based on explicit consent, the vital interests of the child or reasons of substantial public interest (usually safeguarding the child or other individuals).

7.1.10. to provide information to another educational establishment to which a pupil is transferring;

7.1.11. to provide information to the Examination Authority as part of the examination process; and

7.1.12. to provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with

[2] A list of all third parties that we share or that process data on our behalf is also available on the Anglian Learning website. http://anglianlearning.org/governance/

national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

7.2. The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

7.3. The Trust may receive requests from third parties (i.e. those other than the data subject, the Trust, and employees of the Trust) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or the Trust.

7.4. All requests for the disclosure of personal data must be sent to the Data Protection Officer who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

7.5. We disclose personal data about you to the Disclosure and Barring Service for the purposes of carrying out checks on your suitability for work with children.

7.6. We may disclose details about you including national insurance number to our payroll provider to enable you to be paid or to our HR[3].

7.7. We disclose details about our staff, including absence information and allegations to our HR provider for the purposes of HR management. Also, we disclose details about you including contact details and absence information to our Occupational Health Providers to ensure that you are fit for work and that correct support measures are provided, if required[4].

7.8. Where our staff have decided to become part of a salary sacrifice scheme such as that for child care vouchers, we share the personal details with the provider to the extent necessary for them to provide the vouchers to you[5].

7.9. We may share your identity and pay information with HMRC in conjunction with your legal obligation to pay income tax and make national insurance contributions.

---

[3] Our HR and Payroll providers are: Education Personnel Management St Johns House Spitfire Close Ermine Business Park Huntingdon Cambridgeshire PE29 6EP https://www.epm.co.uk/contact/

[4] Pre-employment medicals: Heales Medical 27 Bridge Street Hitchin Hertfordshire SG5 2DF http://www.heales.com/contact.html and Occupational Health referrals: Wrightway Regus House 1010 Cambourne Business Park Cambourne Cambridgeshire CB23 6DP http://www.wrightwayhealth.co.uk/clinics/cambridge/

[5] The vouchers' provider is Computershare, Voucher Service, The Pavilions Bridgwater Road Bristol BS13 8AE https://www.computershare.com/uk/business/other/childcare-vouchers

7.10. We share our staff's details with the pension provider in order to make sure that the staff pays the correct amount and maintain the entitlement to a pension upon retirement. For teachers the scheme is the TPS, for support staff the scheme is LGPS[6].

7.11. The information our staff provided us might be shared to our local authority and the Department for Education (DfE).

7.12. For health and safety reasons, we might also share your information:

- with the Local Authority where necessary for the purpose of identifying individuals that are high risk and vulnerable;
- with Internal teams to ensure that appropriate services and support are provided to those that need it;
- with other Health Organisations and bodies engaged in disease surveillance for the purposes of research, protecting public health, providing appropriate healthcare services to the public and monitoring and managing the Covid-19 outbreak. The information will only be processed and shared in line with the requirements of the Data Protection Act 2018.
  However, in these cases, the information will be held by Anglian Learning until the risk to health posed by COVID-19 has been eliminated and in accordance with Government guidance. Furthermore, If your data is passed to the NHS Test and Trace service in the case of a suspected outbreak, your information will be kept for up to 8 years, as part of the standard contact-tracing period set out by Public Health England.

7.13. The personal data associated with COVID-19 test results will be shared with:

- DHSC, NHS, PHE – to ensure that they can undertake the necessary Test and Trace activities and to conduct research and compile statistical information about Coronavirus.
- Your GP – the NHS may share the information you provide with your GP to maintain your medical records and to offer support and guidance as necessary. Any data you provide to the school will not be shared with your GP.
- Local Government to undertake local public health duties and to record and analyse local spreads.

7.14. Personal Data in the school's COVID-19 test kit log will be shared with DHSC to identify which test kit has been given to which individual in the event of a product recall. The school will not share its internal COVID-19 results register with DHSC.

[6] See https://www.teacherspensions.co.uk/ and https://pensions.cambridgeshire.gov.uk/

7.15. Regarding job applicants, when legally required or necessary, we will share personal information about you to Professional advisers and consultants or Employment and Recruitment Agencies.

7.16. The DfE may also share information about pupils that we give to them, with other people or organisations. Such disclosures could only happen in relation to third parties who promote the education or well-being of children in England by conducting research or analysis, producing statistics, providing information, advice or guidance[7].

7.17. Referring to pupils (both under and over the age of 13), we may make use of limited personal data (such as contact details) relating to pupils, and their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the Trust, but only where consent has been provided to this. We also may transfer information to any association society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to the Trust but only where consent has been obtained first.

8. SUBJECT ACCESS REQUESTS

8.1. Anybody who makes a request to see any personal information held about them by the Trust is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system" (see clause 1.5).

8.2. The individual's full subject access right is to know:

8.2.1. Whether personal data about him or her is being processed

8.2.2. The purpose of the processing

8.2.3. The categories of personal data concerned

8.2.4. The recipients or categories of recipient to whom their personal data has been or will be disclosed

8.2.5. The envisaged period for which the data will be stored or where that is not possible, the criteria used to determine how long the data is stored

8.2.6. The existence of a right to request rectification or erasure of personal data or restriction of processing or to object to the processing

8.2.7. The right to lodge a complaint with the Information Commissioners' Office

[7] For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

8.2.8. Where the personal data is not collected from the individual, any available information as to it's source.

8.2.9. Details of the safeguards in place for any transfers of their data to locations outside the European Economic Area

8.3. All requests should be sent to the Principal of the relevant school within 3 working days of receipt, and must be dealt with in full without delay and at the latest within one month of receipt.

8.4. Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The Principal of the school must, however, be satisfied that:

8.4.1. the child or young person lacks sufficient understanding; and

8.4.2. the request made on behalf of the child or young person is in their interests.

8.5. Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the Trust must have written evidence that the individual has authorised the person to make the application and the Principal of the School must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

8.6. Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

8.7. A Subject Access Request must be made in writing. The Trust may ask for any further information reasonably required to locate the information.

8.8. An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

8.9. All files must be reviewed by the Principal of the School or the CEO for Trust central staff before any disclosure takes place. Access will not be granted before this review has taken place.

8.10. Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

8.11. Any request for any information from the Trust is technically a request under the Freedom of Information Act 2000 (FOI), Anglian Learning being a public authority that has to comply with FOI, whether or not the individual making the request mentions the FOI. However, the ICO has stated that routine requests for information (such as a parent requesting a copy of a policy) can be dealt with outside of the provisions of the Act.

8.12. When considering a request under FOI, the Trust will bear in mind that release under FOI is treated as release to the general public, and so once it has been released to an individual, anyone can then access it, and access cannot be restricted by marking the information "confidential" or "restricted".

8.13. The Trust will respond to requests under FOI as soon as possible, and in any event, within 20 working days of the date of receipt of the request. When calculating the 20 working day deadline, a "working day" is a school day (one in which pupils are in attendance), subject to an absolute maximum of 60 normal working days (not school days) to respond.

9. EXEMPTIONS TO ACCESS BY DATA SUBJECTS

9.1. Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

9.2. There are other exemptions from the right of subject access. If we intend to apply any of them to a request then we will usually explain which exemption is being applied and why.

10. EXEMPTIONS FROM THE RIGHT TO INFORMATION

The followings are considered qualified exemptions from the right to information, according to the Freedom of Information Act 2000:

1. Section 40 (1) – the request is for the applicant's personal data. This will be dealt with under the subject access regime in the Data Protection Act detailed in paragraph 9 of the DPA policy above;

2. Section 40 (2) – compliance with the request would involve releasing third party personal data, and this would be in breach of the DPA principles as set out in paragraph 3.1 of the DPA policy above;

3. Section 41 – information that has been sent to the Trust (but not the Trust's own information) which is confidential;

4. Section 21 – information that is already publicly available, even if payment of a fee is required to access that information;

5. Section 22 – information that the Trust intends to publish at a future date;

6. Section 43 – information that would prejudice the commercial interests of the Trust and / or a third party;

7. Section 38 – information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information);

8. Section 31 – information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras;

9. Section 36 – information which, in the opinion of the Chair of the Trust Board, would prejudice the effective conduct of the Trust. There is a special application form for this on the ICO's website to assist with obtaining of the Chair's opinion

Due to the fact that these exemptions are qualified, the Trust will need to carry out a public interest weighting exercise, balancing the public interest in the information being released, as against the public interest in withholding the information.

11. OTHER RIGHTS OF INDIVIDUALS

11.1. The Trust has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how the Trust will comply with the rights to:

11.1.1. object to processing;

11.1.2. rectification;

11.1.3. erasure; and

11.1.4. data portability.

Right to object to processing

11.2. An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest (grounds 4.5 and 4.6 above) where they do not believe that those grounds are adequately established.

11.3. Where such an objection is made, it must be sent to the Data Protection Officer within 2 working days of receipt, and the Data Protection Officer will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

11.4. The Data Protection Officer shall be responsible for notifying the individual of the outcome of their assessment within 10 working days of receipt of the objection.

Right to rectification

11.5. An individual has the right to request the rectification of inaccurate data without undue delay. Where a request for rectification is received which is not straightforward, it should be sent to the Data Protection Officer within 2 working days of receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

11.6. Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given the option of a review by the CEO, should they be dissatisfied with the outcome, prior to lodging an appeal direct to the Information Commissioner.

11.7. An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure

11.8. Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

11.8.1. where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;

11.8.2. where consent is withdrawn and there is no other legal basis for the processing;

11.8.3. where an objection has been raised under the right to object, and found to be legitimate;

11.8.4. where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);

11.8.5. where there is a legal obligation on the Trust to delete.

11.9. The Data Protection Officer will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to restrict processing

11.10. In the following circumstances, processing of an individual's personal data may be restricted:

11.11. where the accuracy of data has been contested, during the period when the Trust is attempting to verify the accuracy of the data;

11.10.2. where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;

11.10.3. where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;

11.10.4. where there has been an objection made under para 8.2 above, pending the outcome of any decision.

Right to portability

11.12. If an individual wants to send their personal data to another organisation they have a right to request that the Trust provides their information in a structured, commonly used, and machine readable format. As this right is limited to situations where the Trust is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If a request for this is made, it should be forwarded to the Data Protection Officer within 2 working days of receipt, and the Data Protection Officer will review and revert as necessary.

12. BREACH OF ANY REQUIREMENT OF THE GDPR

12.1 Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the Data Protection Officer.

12.2 Once notified, the Data Protection Officer shall assess:

12.2.1 the extent of the breach;

12.2.2 the risks to the data subjects as a consequence of the breach;

12.2.3 any security measures in place that will protect the information;

12.2.4 any measures that can be taken immediately to mitigate the risk to the individuals.

12.3 Unless the Data Protection Officer concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Trust, unless a delay can be justified.

12.4 The Information Commissioner shall be told:

12.4.1 details of the breach, including the volume of data at risk, and the number and categories of data subjects;

12.4.2 the contact point for any enquiries (which shall usually be the Data Protection Officer);

12.4.3 the likely consequences of the breach;

12.4.4 measures proposed or already taken to address the breach.

12.5 If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Data Protection Officer shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

12.6 Data subjects shall be told:

12.6.1 the nature of the breach;

12.6.2 who to contact with any questions;

12.6.3 measures taken to mitigate any risks.

12.7 Data Protection Officer shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Trust Board and a decision made about implementation of those recommendations.

13. COMPLAINTS PROCEDURE

13.1. Complaints concerning the Trust's use of biometric data should be made in writing to the Data Protection Officer.

13.2. Complaints concerning the Trust's use of its CCTV system or the disclosure of CCTV images should be made in writing to the Data Protection Officer. All appeals against the decision of the Data Protection Officer should be made in writing to the CEO.

14. MONITORING COMPLIANCE

14.1. All staff involved in the operation of:

14.1.1. biometric data

14.1.2. the Trust's CCTV System

will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained therein.

14.2. The aforementioned employees with responsibility for accessing, recording, disclosing or otherwise processing such information will be required to undertake data protection training.

15. POLICY REVIEW

15.1. This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed every 3 years.

15.2. However, the Trust's usage of CCTV and the content of this policy shall be reviewed annually by the Data Protection Officer with reference to the relevant legislation or guidance in effect at the time. Further reviews will take place as required.

16. CONTACT

If anyone has any concerns or questions in relation to:
16.1. the policy - contact the CEO.
16.2. the requests of information - direct them in the first instance to Data Protection Officer.
16.3. the processing of personal information – contact the Data Protection Officer (and in case of a dissatisfactory result, raise a complaint with the Information Commissioner's Office: Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF).
16.4. any of the rights a job applicant has – contact the Data Protection Officer, Mark Povey, at <mark@js-ig.com>.
16.5. the copy of information held about students over 13 years old or a volunteer – contact the relevant school

SECTION II. SPECIAL PROVISIONS

1. BIOMETRIC DATA PROCEDURES

1.1. The Trust ensures that each parent of a child is notified of the option to log biometric data as part of an automated biometric recognition system for their child to access their account.

1.2. The parents are provided with full information as to the alternatives that are available should they wish not to provide consent.

1.3. The written consent of at least one parent/carer must be obtained before the data are taken from the child and used (i.e. 'processed' – see 3 below). This applies to all pupils in schools and colleges under the age of 18. In no circumstances can a child's biometric behaviour be processed without written consent.

1.4. Should one parent/carer provide written consent and another parent/carer object then the biometric data will not be taken or will be destroyed

1.5. For new pupils year 7 onwards, prior to the biometric data being taken it will be verbally explained to them as to what their parents have consented to and they will also be requested to provide written consent. Should they object then the biometric information will not be taken.

1.6. At the start of each academic year the form teacher will explain to their pupils that they have a right to withdraw consent should they wish to with regards to biometric data and if any pupil expresses a wish to do so then the data will be destroyed.

1.7. Should the Trust wish to use the biometric data for any other purpose than that of operating the pupils account for catering then parents and the pupils will be informed and a fresh consent will be sought from the parent and the pupil.

1.8. All biometric data will be immediately destroyed once the pupil leaves the school.

2. CCTV SURVEILLANCE SYSTEMS

2.1. CCTV SYSTEMS OVERVIEW

2.1.1. The CCTV systems are owned by the Trust and managed by the Trust and its appointed agents, which include any management or maintenance companies that may be appointed. Under the Data Protection Act 2018 and GDPR, the Trust is the 'data controller' for the images produced by the CCTV system.

2.1.2. The Director of ICT is responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.

2.1.3. The CCTV systems operate across all of the sites. Details of the number of cameras and their location can be obtained by contacting the Director of ICT.

2.1.4. Signs are placed at relevant points to inform people that CCTV cameras are operational in that area.

2.1.5. The Director of Operations is responsible for ensuring that adequate signage is erected in compliance with the ICO CCTV Code of Practice.

2.1.6. Cameras are sited to ensure that they cover Trust premises as far as is possible. Cameras are installed throughout the Trust's sites within buildings and externally in vulnerable public facing areas.

2.1.7. Cameras are primarily sited to focus on communal areas of the school sites, but may also be used in rooms for the protection of people and assets, where considered necessary by the Principal and subject to a Privacy Impact Assessment being conducted.

2.1.8. Where cameras are within sight of private areas, such as residential, the use of 'privacy masks' is implemented, such that privacy in these physical areas can be maintained

2.1.9. The CCTV system is operational and is capable of being monitored for 24 hours a day, every day of the year.

2.1.10. Any proposed new CCTV installation is subject to a Privacy Impact Assessment.

2.2. PURPOSES OF THE CCTV SYSTEMS

2.2.1. The main purposes are:

- the prevention, reduction, detection and investigation of crime and other incidents;
- ensuring the safety of staff, students and visitors;
- assisting in the investigation of suspected breaches of Trust regulations by staff or students
- observing the Trust's sites and areas under surveillance in order to identify incidents requiring a response (whilst any response should be proportionate to the incident being witnessed)

2.2.2. Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose or for purposes of entertainment.

2.3. MONITORING AND RECORDING

2.3.1. Cameras are monitored by the Site Team, Behaviour Team and selected members of the Senior Leadership Teams. Where specifical operations are in place, such as Sports Centres, access to relevant camera feeds to these personnel is provided. The system is supported by the Director of Operations and Technical Services Team.

2.3.2. Images are recorded centrally on servers located securely in the school and are viewable by the CCTV users listed in 2.3.1, section II. Additional staff may be authorised by the Headteacher of the school to monitor cameras sited within their own areas of responsibility on a view only basis.

2.3.3. The cameras installed provide images that are of suitable quality for the specified purposes for which they are installed and the cameras are checked regularly to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images is accurate.

2.3.4. All images recorded by the CCTV System remain the property and copyright of the Trust.

2.3.5. The monitoring of staff activities will be carried out in accordance with Part 3 of the Employment Practices Code (ICO).

2.3.6. The use of covert cameras will be restricted to very rare occasions, when a series of criminal acts have taken place within a particular area that is not otherwise fitted with CCTV. A request for the use of covert cameras will clearly state the purpose and reasons for use and the authority of the Chief Executive Officer will be sought before the installation of any covert cameras. The CEO should be satisfied that all other physical methods of prevention have been exhausted prior to the use of covert recording.

2.3.7. All such monitoring will be fully documented and will only take place for a limited and reasonable period.

2.4. DISCLOSURE OF IMAGES

2.4.1. Additional to point 9 of the section I, a record of any disclosure made under this policy will be held on the CCTV management system, itemising the date, time, camera, requestor, authoriser and reason for the disclosure.

2.4.2. A request for images made by a third party should be made in writing to the Headteacher. The Police may request images verbally as part of an investigation but the request must be logged by the academy.

2.4.3. In limited circumstances, it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation.

2.4.4. Such disclosures will be made at the direction of the Headteacher of the academy in question or Director of ICT, with reference to relevant legislation and where necessary, following advice from the DPO.

2.4.5. Where an allegation has been raised against a member of staff and at the formal request of the Investigating Officer or HR Manager/Advisor, the Director of ICT may provide access to CCTV images as part of the investigation.

2.4.6. The Director of ICT may provide access to CCTV images to Investigating Officers when sought as evidence in relation to allegations of pupil behaviour.

2.4.7. A record of any disclosure made under this policy will be held on the CCTV management system, itemising the date, time, camera, requestor, authoriser and reason for the disclosure.

2.5. **RETENTION OF IMAGES**

2.5.1. Unless required for evidential purposes, the investigation of an offence or as required by law, CCTV will be retained for no longer than 30 days from the date of recording. Images will be automatically overwritten after this point.

2.5.2. Where an image is required to be held in excess of the retention period referred to in 2.5.1, the Headteacher or their nominated deputy, will be responsible for authorising such a request.

2.5.3. Images held in excess of their retention period will be reviewed on a three monthly basis and any not required for evidential purposes will be deleted.

2.5.4. Access to retained CCTV images is restricted to the Director of ICT and/or Headteacher of the academy and other persons as required and as authorised by the Director of ICT or Headteacher.

2.6. **AUDIO RECORDINGS**

2.6.1. The Trust may use cameras to record audio as well as images in certain locations where staff and students may feel particularly vulnerable. Such recordings will only be accessed should there an incident where verbal abuse etc has been alleged. Recordings will not be accessed for the purpose of listening to normal everyday conversations.

2.6.2. Written permission by the Headteacher of the school is required prior to any member of staff accessing the audio recordings.

3. DOCUMENT RETENTION AND DESTRUCTION

3.1. For information about the categories of documents we keep and their retention period, please check the Document Retention Policy. Moreover, where we have decided to keep information longer than the statutory requirement, this has been explained within the aforementioned policy.

3.2. The CEO shall be responsible for ensuring the destruction procedure for documents at the end of their retention period is carried out appropriately and delegating responsibilities, and any questions regarding this policy should be referred to them.

3.3. If a document or piece of information is reaching the end of its stated retention period, but you are of the view that it should be kept longer, please refer to the CEO who will make a decision as to whether it should be kept, for how long, and note the new time limit and reasons for extension.

3.4. The deletion of documents (including the automatic deletion process) at the end of the retention period is explained within the Document Retention Policy.

4. PROCEDURE ON REQUESTS FOR INFORMATION

4.1. When a request is received that cannot be dealt with by simply providing the information, it should be referred in the first instance to the Principal of the relevant school, who may re-allocate to an individual with responsibility for the type of information requested.

4.2. The first stage in responding is to determine whether or not the Trust "holds" the information requested. The Trust will hold the information if it exists in computer or paper format. Some requests will require the Trust to take information from different sources and manipulate it in some way. Where this would take minimal effort, the Trust is considered to "hold" that information, but if the required manipulation would take a significant amount of time, the requestor should be

contacted to explain that the information is not held in the manner requested, and offered the opportunity to refine their request. For example, if a request required the Trust to add up totals in a spread sheet and release the total figures, this would be information “held” by the Trust. If the Trust would have to go through a number of spread sheets and identify individual figures and provide a total, this is likely not to be information “held” by the Trust, depending on the time involved in extracting the information.

4.3. The second stage is for the Trust to decide whether the information can be released, or whether one of the exemptions set out in the Act applies to the information (see point 10 and 11, section I).

4.4. When responding to a request where the Trust has withheld some or all of the information, the Trust will explain why the information has been withheld, quoting the appropriate section number and explaining how the information requested fits within that exemption. If the public interest test has been applied, this also needs to be explained.

4.5. The letter should end by explaining to the requestor how they can complain – either by reference to an internal review by a Trustee, or by writing to the ICO.