Data Protection and Information Security Policy

July 2025

Written By:	Claire Murton – Head of Operations
Governing Committee Responsible	Board of Trustees
Approved By and Date:	Main Trust Board July 2025
Monitored & Reviewed By and Date	Roger Simmons (Data Protection Officer) July 2023
Date of Next Review	MTB - July 2027
SLT Responsible for Monitoring & Review	Peter Hall – Assistant Headteacher Theo Richards – Deputy Headteacher

Contents:

Statement of intent

MARK Education Trust is required to keep and process certain information about its staff members and students in accordance with its legal obligations under the UK GDPR.

The trust may, from time to time, be required to share personal information about its staff or students with other organisations, mainly the Local Authority (LA), other trusts and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and trustees are aware of their responsibilities and outlines how the trust complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and MARK Education Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- DFE Keeping Children Safe in Education

1.2. This policy also has regard to the following guidance:

- ICO (2022) 'Guide to the General Data Protection Regulation (GDPR)'
- ICO (2012) IT Asset disposal for organisations
- DfE (2023) Data Protection in Schools

1.3. This policy will be implemented in conjunction with the following other trust policies:

- Photography and Video Policy
- Freedom of Information Policy
- CCTV Policy
- Child Protection and Safeguarding Policy
- Data Retention Schedule Policy

2. Applicable data

2.1. For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

2.2. 'Sensitive personal data' is referred to in the UK GDPR as 'special categories of personal data', and is defined as:

- Genetic data.
- Biometric data.
- Data concerning health.
- Data concerning a person's sex life.
- Data concerning a person's sexual orientation.
- Personal data which reveals:
- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.

2.3. 'Sensitive personal data' does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, schools are only able to process this if it is either:

- Under the control of official authority; or
- Authorised by domestic law.

2.4. The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below:

2.5. The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health and research

3. Principles

3.1. In accordance with the requirements outlined in the UK GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- 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; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- 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

3.2. The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

3.3. The Privacy Notice for students and parents is available on the trust website. The Privacy Notice for staff, volunteers and trustees are issued and available internally.

4. Accountability

4.1. MARK Education Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR.

4.2. The trust will provide comprehensive, clear and transparent Privacy Notices.

4.3. Records of activities relating to higher risk processing will be maintained, such as the processing of activities that:

- Are not occasional
- Could result in a risk to the rights and freedoms of individuals
- Involve the processing of special categories of data or criminal conviction and offence data

4.4. Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

4.5. The academy will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation
- Transparency
- Allowing individuals to monitor processing
- Continuously creating and improving security features

4.6. Data Protection Impact Assessments will be used, where appropriate.

5. Data protection officer (DPO)

5.1. A DPO has been appointed in order to:

- Inform and advise the trust and its employees about their obligations to comply with the UK GDPR and other data protection laws
- Monitor the trust's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members

5.2. Our DPO is Roger Simmons, GDPR Practitioner and DPO, 07704-838512 rsimmonsltd@gmail.com

5.3. The DPO will report to the highest level of management at the trust, which is the Executive Headteacher.

5.4. The DPO will operate independently and will not be dismissed or penalised for performing their task.

5.5. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

6. Lawful processing

6.1. The legal basis for processing data will be identified and documented prior to data being processed.

6.2. Under the UK GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
  - Compliance with a legal obligation
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
  - For the performance of a contract with the data subject or to take steps to enter into a contract
  - Protecting the vital interests of a data subject or another person
  - For the purposes of legitimate interests pursued by the controller or a third party, except in some limited cases where such interests are overridden by the interests, rights or freedoms of the data subject

6.3. Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
  - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with article 89(1)

7. Consent

7.1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

7.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

7.3. Where consent is given, a record will be kept documenting how and when consent was given.

7.4. The trust ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

7.5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be re-obtained.

7.6. Consent can be withdrawn by the individual at any time.

7.7. Where the school opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined in 7.2, the school obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children.

7.8. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, considering the requirements outlined in 7.2.

8. The right to be informed

8.1. The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

8.2. If services are offered directly to a child, the trust will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

8.3. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO
- The purpose of, and the legal basis for, processing the data
- The legitimate interests of the controller or third party
- Any recipient or categories of recipients of the personal data
- Details of transfers to third countries and the safeguards in place
- The retention period of criteria used to determine the retention period
- The existence of the data subject's rights, including the right to:
  - Withdraw consent at any time
  - Lodge a complaint with a supervisory authority
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences

8.4. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as

well as any possible consequences of failing to provide the personal data, will be provided.

8.5. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the trust holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

8.6. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

8.7. In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed
- If the data are used to communicate with the individual, at the latest, when the first communication takes place

9. The right of access

9.1. Individuals have the right to obtain confirmation that their data is being processed.

9.2. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

9.3. The trust will verify the identity of the person making the request before any information is supplied.

9.4. The information may be provided in a commonly used electronic format.

9.5. All requests will be responded to without delay and at the latest, within one month of receipt.

9.6. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

9.7. Where a request is manifestly unfounded or excessive, the trust holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

9.8. In the event that a large quantity of information is being processed about an individual, the trust will ask the individual to specify the information the request is in relation to.

10. The right to rectification

10.1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.

10.2. Where the personal data in question has been disclosed to third parties, the trust will inform them of the rectification where possible.

10.3. Where appropriate, the trust will inform the individual about the third parties that the data has been disclosed to.

10.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

10.5. Where no action is being taken in response to a request for rectification, the trust will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

11. The right to erasure

11.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

11.2. Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

11.3. The trust has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

11.4. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

11.5. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

11.6. Where personal data has been made public within an online environment, the trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

12. The right to restrict processing

12.1. Individuals have the right to block or suppress the trust's processing of personal data.

12.2. In the event that processing is restricted, the trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

12.3. The trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the trust has verified the accuracy of the data
- Where an individual has objected to the processing and the trust is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

12.4. If the personal data in question has been disclosed to third parties, the trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

12.5. The trust will inform individuals when a restriction on processing has been lifted.

13.The right to data portability

13.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

13.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

13.3. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

13.4. Personal data will be provided in a structured, commonly used and machine-readable form.

13.5. The trust will provide the information free of charge.

13.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

13.7. The trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

13.8. In the event that the personal data concerns more than one individual, the trust will consider whether providing the information would prejudice the rights of any other individual.

13.9. The trust will respond to any requests for portability within one month.

13.10. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

13.11. Where no action is being taken in response to a request, the trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14. The right to object

14.1. The trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

14.2. Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics

14.3. Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation
- The trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual

14.4. Where personal data is processed for direct marketing purposes:

- The trust will stop processing personal data for direct marketing purposes as soon as an objection is received
- The trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes

14.5. Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object
- Where the processing of personal data is necessary for the performance of a public interest task, the trust is not required to comply with an objection to the processing of the data

14.6. Where the processing activity is outlined above, but is carried out online, the trust will offer a method for individuals to object online.

15. Automated decision making and profiling

15.1. Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling
- It produces a legal effect or a similarly significant effect on the individual

15.2. The trust will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

15.3. When automatically processing personal data for profiling purposes, the trust will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact
- Using appropriate mathematical or statistical procedures
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects

15.4. Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The trust has the explicit consent of the individual
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law

16. Privacy by design and privacy impact assessments

16.1. The trust will act in accordance with the UK GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the trust has considered and integrated data protection into processing activities.

16.2. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the trust's data protection obligations and meeting individuals' expectations of privacy.

16.3. DPIAs will allow the trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the trust's reputation which might otherwise occur.

16.4. A DPIA will be carried out by the DPO when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

16.5. A DPIA will be used for more than one project, where necessary.

16.6. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling

- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV

16.7. The trust will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

16.8. Where a DPIA indicates high risk data processing, the trust's DPO will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

17. Data in transit

17.1. All employees, trustees and volunteers are personally responsible for taking reasonable and appropriate precautions to ensure that all sensitive and confidential data is protected within the trust and when accessed or transported outside the trust.

17.2. All sensitive and confidential electronic data being taken outside of its normally secure location must be encrypted. All non-electronic data must be transported and stored using an appropriate level of care and security.

17.3. Data in transit should be kept to the minimum amount required to undertake the school's responsibilities.

17.4. Any data loss must be reported immediately to the Executive Headteacher. Disciplinary action could be taken where employees do not follow the guidance set out in this policy.

18.Protection of biometric information

18.1. The DfE provide guidance on the Protection of biometric information of children in schools and colleges under Protection of Freedoms Act 2012 and Data Protection Act 2018.

18.2. The written consent of at least one parent must be obtained before the biometric data is taken from the child and used. This applies to all students in schools and colleges under the age of 18.

18.3. In no circumstances can a child's biometric data be processed without written consent. The trust will not process the biometric data of a student (under 18 years of age) where:

a) the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;

b) no parent has consented in writing to the processing; or

c) a parent has objected in writing to such processing, even if another parent has given written consent.

18.4. The trust will where possible provide reasonable alternative means of accessing services for those students who will not be using an automated biometric recognition system.

18.5. The latest guidance published by the DfE for the implementation of this aspect of policy is available via the following link:

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

19. Data breaches

19.1. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

19.2. The Executive Headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

19.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

19.4. All breaches will be recorded on the trust's Breach Management Form and signed-off by the DPO once resolved. Any notifiable breaches will be reported, by the DPO, to the relevant supervisory authority within 72 hours of the trust becoming aware of it.

19.5. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

19.6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the trust will notify those concerned directly.

19.7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

19.8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

19.9. Effective and robust breach detection, investigation and internal reporting procedures are in place at the trust, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

19.10. Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

19.11. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

20. Data security

20.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

20.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

20.3. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

20.4. Memory sticks will not be used to hold personal information.

20.5. All electronic devices are password-protected to protect the information on the device in case of theft.

20.6. Where possible, the trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.

20.7. Staff and trustees will not store personal data on their personal laptops, computers or devices. Staff and trustees may access data online via their secure office365 login or via a remote desktop connection to our system. For the purposes of this statement Personal Data refers to data collected by, or obtained on behalf of, MARK Education Trust.

20.8. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

20.9. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

20.10. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

20.11. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the trust premises accepts full responsibility for the security of the data.

20.12. Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

20.13. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the trust containing sensitive information are supervised at all times.

20.14. The physical security of the trust's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

20.15. MARK Education Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

20.16. The Head of IT is responsible for continuity and recovery measures are in place to ensure the security of protected data.

21. Publication of information

21.1. MARK Education Trust publishes a publication scheme on its website outlining classes of information that will be made routinely available following a Freedom of Information request, including:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

21.2. Classes of information specified in the publication scheme are made available quickly and easily on request.

21.3. A Guide to Information is available as an appendix in the Freedom of Information policy and also separately on the website.

21.4. MARK Education Trust will not publish any personal information, including photos, on its website without the permission of the affected individual.

21.5. When uploading information to the trust website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

22. CCTV and photography

22.1. The trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

22.2. The trust notifies all students, staff and visitors of the purpose for collecting CCTV images via CCTV signage and notice boards, letters and email.

22.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. The location of cameras is discussed by the Senior Leadership Team. The view from new cameras is checked by the IT staff to ensure it captures only the view intended.

22.4. All CCTV footage will be kept no more than 30 days for security purposes; the Head of IT is responsible for keeping the records secure and allowing access.

22.5. The trust will always indicate its intentions for taking photographs of students and will retrieve permission before publishing them.

22.6. If the trust wishes to use images/video footage of students in a publication, such as the trust website, prospectus, or recordings of trust plays, written permission will be sought for the particular usage from the parent of the student.

22.7. Precautions, as outlined in the Photography and Videos at Trust Policy, are taken when publishing photographs of students, in print, video or on the trust website.

22.8. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

23. Data retention

23.1. The academy has a Data Retention Policy that is reviewed every two years.

23.2. Data will not be kept for longer than is necessary and unrequired data will be deleted as soon as practicable.

23.3. Some educational records relating to former students or employees of the trust may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

23.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

24. DBS data

24.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

24.2. Data provided by the DBS will never be duplicated.

24.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

25. The Regulator

25.1. The Information Commissioner's Office is responsible for:

- Overseeing compliance with Data Protection legislation
- Supporting organisations to become compliant
- Enforcing the legal processing of data
- Investigating complaints where organisations are not compliant

25.2. The trust must register with the ICO and maintain a current record of the information it is processing, the legal basis for processing the information and who it is being shared with. The trust's ICO Registration Reference is Z3587412.

25.3. Office of the Information Commissioner can be contacted as follows:

The Information Commissioners, Wycliffe House, Water Lane
Wilmslow, Cheshire, SK9 5AF website: www.ico.gov.uk

26. Monitoring and Review

26.1. This policy will be regularly monitored by the external DPO, the delegated SLT DPO links and the Head of Operations to ensure it is meeting statutory requirements.

26.2. The next scheduled review date by the board of trustees is July 2027.