



Data Protection Policy

Author	Trust HR Team
Date of issue	27/03/2025
Date ratified	26/03/2025
Date for review	Autumn Term 2025-26

DOCUMENT CONTROL

Unless there are legislative or regulatory changes in the interim, this policy will be reviewed annually. Should no substantive changes be required at that point, the policy will move to the next review cycle.

Version	Date	Changes
1.0	02/2025	<ul style="list-style-type: none">• Transferred to new template• Added section on Artificial Intelligence (AI)



Contents

Part 1 – Introduction	4
1. Aims	4
2. Legislation and guidance	4
3. Definitions	4
4. Data Protection Principles.....	5
Part 2 – Organisational Arrangements	5
5. The Data Controller	5
6. Roles and responsibilities	5
Part 3 – Data Management	6
7. Collecting personal data	6
8. Limitation, minimisation and accuracy	7
9. Sharing personal data	8
10. Subject access requests and other rights of individuals	8
11. Biometric recognition systems	10
12. CCTV	10
13. Photographs and videos.....	10
14. Artificial Intelligence (AI)	11
15. Data Protection by Design and Default	11
16. Data Security and Storage of Records	11
17. Disposal of records.....	12
18. Personal data breaches	12
19. Training	12
20. Monitoring arrangements	12
21. Appendix 1	13
22. Appendix 2	15

Part 1 – Introduction

1. Aims

- 1.1. Mercia Learning Trust (“our trust”) aims to ensure that all personal data collected about employees, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.
- 1.2. This policy applies to all personal data, regardless of whether it is in paper or electronic format, and describes how that personal data must be collected, handled and stored to meet our trust’s data protection standards and to comply with the law.

2. Legislation and guidance

- 2.1. This policy meets the requirements of the UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 and Data Protection Act 2018 (DPA 2018). It is based on guidance published by the Information Commissioner’s Office (ICO) on the GDPR.
- 2.2. It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.
- 2.3. It also reflects the ICO’s Code of Practice for the use of surveillance cameras and personal information.
- 2.4. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child’s educational record.
- 2.5. Furthermore, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	<p>Any information relating to an identified, or identifiable, individual. This may include the individual’s:</p> <ul style="list-style-type: none">• name (including initials)• address and contact details• identification numbers such as NI or passport numbers• location data• online identifier, such as a username• photographs or video footage
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual’s:</p> <ul style="list-style-type: none">• racial or ethnic origin• political opinions• religious or philosophical beliefs• trade union membership• genetics• biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes• health – physical or mental• sex life or sexual orientation
Processing	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
Data subject	<p>The identified or identifiable individual whose personal data is held or processed.</p>

Term	Definition
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Data Protection Officer (DPO)	A named individual who helps our trust to protect their data and stay compliant with data protection regulations.
Information Commissioner's Office (ICO)	The UK supervisory authority for data protection. They have the responsibility for enforcing the data protection regulations (GDPR).
GDPR	The General Data Protection Regulations 2016. New regulations covering data protection that became enforceable in May 2018.

4. Data Protection Principles

- 4.1. The UK GDPR is based on data protection principles that our trust must comply with.
- 4.2. The principles say that personal data must be:
 - 4.2.1. processed lawfully, fairly and in a transparent manner.
 - 4.2.2. collected for specified, explicit and legitimate purposes.
 - 4.2.3. adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
 - 4.2.4. accurate and, where necessary, kept up to date.
 - 4.2.5. kept for no longer than is necessary for the purposes for which it is processed.
 - 4.2.6. processed in a way that ensures it is appropriately secure.
- 4.3. This policy sets out how our trust aims to comply with these principles.

Part 2 – Organisational Arrangements

5. The Data Controller

- 5.1. Our trust processes personal data relating to parents, pupils, employees, governors, visitors and others, and therefore is a data controller.
- 5.2. Our trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

6. Roles and responsibilities

- 6.1. This policy applies to all employees and volunteers working for our trust. Employees who do not comply with this policy may face disciplinary action.
- 6.2. Trust Board**
- 6.3. Our Trust Board has overall responsibility for ensuring that our trust complies with all relevant data protection obligations.
- 6.4. Data Protection Officer**
- 6.5. The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.
- 6.6. They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on trust data protection issues.
- 6.7. The DPO is also the first point of contact for individuals whose data our trust processes, and for the ICO.

- 6.8. Our DPO is GDPRiS but any GDPR related query should be sent to dataprotection@merciatrust.co.uk in the first instance.
- 6.9. The headteacher is responsible for day-to-day data protection matters in our schools.
- 6.10. CEO/Headteacher**
- 6.11. The headteacher acts as the representative of the data controller on a day-to-day basis.
- 6.12. Schools**
- 6.13. Schools are responsible for carrying out continuous audits and reviews of the data processed in the schools using our trust's auditing systems (currently GDPRiS). This process helps the schools and our trust to identify and mitigate any risks in data processes.
- 6.14. Employees**
- 6.15. All employees are responsible for:
- 6.15.1. collecting, storing and processing any personal data in accordance with this policy.
 - 6.15.2. informing our trust of any changes to their personal data, such as a change of address.
 - 6.15.3. contacting the DPO in the following circumstances:
 - 6.15.3.1. with any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
 - 6.15.3.2. if they have any concerns that this policy is not being followed.
 - 6.15.3.3. if they are unsure whether they have a lawful basis to use personal data in a particular way.
 - 6.15.3.4. if they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK.
 - 6.15.3.5. if there has been a data breach.
 - 6.15.3.6. whenever they are engaging in a new activity that may affect the privacy rights of individuals.
 - 6.15.3.7. if they need help with any contracts or sharing personal data with third parties.

Part 3 – Data Management

7. Collecting personal data

7.1. Privacy Notices

- 7.2. Our trust has privacy notices for the following groups which outline the information above that is specific to them:
- 7.2.1. Employees
 - 7.2.2. Governors and volunteers
 - 7.2.3. Job applicants
 - 7.2.4. Parents
 - 7.2.5. Pupils
- 7.3. There may be circumstances where it is considered necessary to process personal data or special category personal data to protect the vital interests of a data subject. This may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the DPO will be consulted, and a decision made only after seeking further clarification.
- 7.4. Where the school relies on:
- 7.4.1. 'Performance of contract' to process a pupil's data, the school considers the pupil's competence to understand what they are agreeing to, and to enter into a contract.
 - 7.4.2. 'Legitimate interests' to process a pupil's data, the school takes responsibility for identifying the risks and consequences of the processing and puts age-appropriate safeguards in place.
 - 7.4.3. Consent to process a pupil's data, the school ensures that the requirements outlined in section 6 are met, and the school does not exploit any imbalance of power in the relationship between the school and the pupil.

7.5. Lawfulness, fairness and transparency

- 7.6. We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:
- 7.6.1. The data needs to be processed so that our trust can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract.
 - 7.6.2. The data needs to be processed so that our trust can **comply with a legal obligation**.
 - 7.6.3. The data needs to be processed to ensure the **vital interests** of the individual eg. to protect someone's life.
 - 7.6.4. The data needs to be processed so that our trust, as a public authority, can perform a task **in the public interest**, and carry out its official functions.
 - 7.6.5. The data needs to be processed for the **legitimate interests** of our trust or a third party (provided the individual's rights and freedoms are not overridden).
 - 7.6.6. The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**.
- 7.7. For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:
- 7.7.1. The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent.
 - 7.7.2. The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law.
 - 7.7.3. The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
 - 7.7.4. The data has already been made manifestly public by the individual.
 - 7.7.5. The data needs to be processed for the establishment, exercise or defence of legal claims.
 - 7.7.6. The data needs to be processed for reasons of substantial public interest as defined in legislation.
 - 7.7.7. The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
 - 7.7.8. The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
 - 7.7.9. The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.
- 7.8. For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:
- 7.8.1. the individual (or their parent/carer when appropriate in the case of a pupil) has given consent.
 - 7.8.2. the data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent.
 - 7.8.3. the data has already been made manifestly public by the individual.
 - 7.8.4. the data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights.
 - 7.8.5. the data needs to be processed for reasons of substantial public interest as defined in legislation.
- 7.9. Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.
- 7.10. We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.
- 7.11. Further details of our processing of special category data can be found in the Appropriate Policy Document at Appendix 2.

8. Limitation, minimisation and accuracy

- 8.1. We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
- 8.2. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

- 8.3. Employees must only process personal data where it is necessary to do their jobs.
- 8.4. We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.
- 8.5. When employees no longer need the personal data they hold, they must ensure it is deleted, destroyed or anonymised. This will be done in accordance with our trust's retention schedule.

9. Sharing personal data

- 9.1. We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:
 - 9.1.1. there is an issue with a pupil or parent/carers that puts the safety of our employees at risk.
 - 9.1.2. we need to liaise with other agencies – we will seek consent as necessary before doing this.
 - 9.1.3. our suppliers or contractors need data to enable us to provide services to our employees and pupils – for example, IT companies. When doing this, we will:
 - 9.1.3.1. only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
 - 9.1.3.2. establish a contract with the supplier or contractor, to ensure the fair and lawful processing of any personal data we share.
 - 9.1.3.3. only share data that the supplier or contractor needs to carry out their service.
- 9.2. We may also share personal data with law enforcement and government bodies where we are legally required to do so.
- 9.3. We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or employees.
- 9.4. Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

10. Subject access requests and other rights of individuals

10.1. Subject access requests

- 10.2. Individuals have a right to make a 'subject access request' to gain access to personal information that our trust holds about them. This includes:
 - 10.2.1. confirmation that their personal data is being processed.
 - 10.2.2. access to a copy of the data.
 - 10.2.3. the purposes of the data processing.
 - 10.2.4. the categories of personal data concerned.
 - 10.2.5. who the data has been, or will be, shared with.
 - 10.2.6. how long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
 - 10.2.7. the source of the data, if not the individual.
 - 10.2.8. whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
 - 10.2.9. the safeguards provided if the data is being transferred internationally.
- 10.3. Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include the following information:
 - 10.3.1. name of individual.
 - 10.3.2. correspondence address.
 - 10.3.3. contact number and email address.
 - 10.3.4. details of the information requested.
- 10.4. If employees receive a subject access request, they must immediately forward it to the Designated Data Protection Lead in their school and alert the headteacher.

10.5. Children and subject access requests

- 10.6. Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.
- 10.7. Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our schools may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

10.8. Responding to subject access requests

- 10.9. When responding to requests, we:
 - 10.9.1. may ask the individual to provide 2 forms of identification.
 - 10.9.2. may contact the individual via phone to confirm the request was made.
 - 10.9.3. will respond without delay and within 1 month of the request (or receipt of the additional information needed to confirm identity, where relevant).
 - 10.9.4. will provide the information free of charge.
 - 10.9.5. may tell the individual we will comply within 3 months of receipt of the request where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.
- 10.10. We will not disclose information if it:
 - 10.10.1. might cause serious harm to the physical or mental health of the pupil or another individual.
 - 10.10.2. would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
 - 10.10.3. would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent, and it would be unreasonable to proceed without it.
 - 10.10.4. is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.
- 10.11. If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee that takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.
- 10.12. When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

10.13. Other data protection rights of the individual

- 10.14. In addition to the right to make a subject access request and the right to receive information when we are collecting their data about how we use and process it, individuals also have the right to:
 - 10.14.1. withdraw their consent to processing at any time.
 - 10.14.2. ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).
 - 10.14.3. prevent use of their personal data for direct marketing.
 - 10.14.4. challenge processing which has been justified on the basis of public interest, official authority or legitimate interests.
 - 10.14.5. challenge decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them).
 - 10.14.6. be notified of a data breach in certain circumstances.
 - 10.14.7. make a complaint to the ICO.
 - 10.14.8. ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).
- 10.15. Individuals should submit any request to exercise these rights to the Designated Data Protection Lead in the school. If employees receive such a request, they must immediately forward it to the Designated Data Protection Lead in their school and alert the headteacher and trust data protection lead.

10.16. Parental requests to see the educational record.

- 10.17. Those with parental responsibility can request access to a child's education record under education regulations.
- 10.18. An education record covers information that comes from a teacher or other employee of a local authority or school, the pupil, or a parent, and is processed by or for the school's governing body or teacher. This is likely to cover information such as the records of the pupil's academic achievements, attendance and behaviour as well as correspondence from teachers or Local Authority employees such as educational psychologists engaged by the school. It may also include information from the child and from parents, carers or guardians. Information provided by the parent of another child or information created by a teacher solely for their own use would not form part of a child's education record.
- 10.19. There is no automatic parental right of access to educational records in academies. However, our trust has determined that parents, or those with parental responsibility, can have access to their child's educational record within 15 school days of receipt of a written request.
- 10.20. Access to education records is a separate right under the Education (Pupil Information) (England) Regulations 2005 and is not covered by Data Protection legislation. Unlike the right to access under Data Protection legislation, this right does not extend to pupils.

11. Biometric recognition systems

- 11.1. Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash) we will comply with the requirements of the Protection of Freedoms Act 2012.
- 11.2. Parents and carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. Our schools will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.
- 11.3. Parents, carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.
- 11.4. Parents, carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.
- 11.5. As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s) or carer(s).
- 11.6. Where employees or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Employees and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

- 12.1. We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV.
- 12.2. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.
- 12.3. Any enquiries about the CCTV system should be directed to the school office.

13. Photographs and videos

- 13.1. As part of our school activities, we may take photographs and record images of individuals within our schools.
- 13.2. Uses may include:
- 13.2.1. within school on notice boards and in school magazines, brochures, newsletters, etc.
 - 13.2.2. outside of school by external agencies such as the school photographer, newspapers or local university following an event.
 - 13.2.3. online on our school website or social media pages.
- 13.3. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.
- 13.4. Parents, or pupils aged 13 and over, can opt out of images being taken for promotional or online purposes by submitting a written request to the school office. If you opt out, we will delete the photograph or video and not distribute it further.

14. Artificial Intelligence (AI)

- 14.1. Artificial intelligence (AI) tools are now widespread and easy to access. Employees, pupils and parents and carers may be familiar with generative tools such as ChatGPT, Microsoft Co-Pilot and Google Gemini. Our trust supports the use of AI to reduce workload and recognises that AI can support inclusive practice and enhance teaching and learning but that it also poses a risk to sensitive and personal data.
- 14.2. To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.
- 14.3. If personal and/or sensitive data is entered into an unauthorised generative AI tool, our trust will treat this as a data breach and will follow the personal data breach procedure outlined in Appendix 1.

15. Data Protection by Design and Default

- 15.1. We will put measures in place to show that we have integrated data protection into all our data processing activities, including:
 - 15.1.1. appointing a suitably qualified DPO and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
 - 15.1.2. only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law.
 - 15.1.3. completing data protection impact assessments (DPIA) where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
 - 15.1.4. integrating data protection into internal documents including this policy, any related policies and privacy notices.
 - 15.1.5. regularly training employees on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
 - 15.1.6. regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
 - 15.1.7. appropriate safeguards being put in place if we transfer any personal data outside the UK where different data protection laws will apply.
 - 15.1.8. maintaining records of our processing activities, including:
 - 15.1.8.1. for the benefit of data subjects, making available the name and contact details of our school data lead and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).
 - 15.1.8.2. for all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

16. Data Security and Storage of Records

- 16.1. We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
- 16.2. In particular:
 - 16.2.1. paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
 - 16.2.2. papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
 - 16.2.3. where personal information needs to be taken off site, employees must sign it in and out from the school office.
 - 16.2.4. passwords that are at least 6 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Employees and pupils are reminded to change their passwords at regular intervals.
 - 16.2.5. security software is used to protect all portable devices such as laptops. Two factor authentication is in place when employees access our trust's network remotely.
 - 16.2.6. employees or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Acceptable Use of IT Policy).

- 16.2.7. where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

17. Disposal of records

- 17.1. Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely where we cannot or do not need to rectify or update it.
- 17.2. For example, we will shred or incinerate paper-based records and delete electronic files. We may also use a third party to safely dispose of records on our trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal data breaches

- 18.1. Our trust will make all reasonable endeavours to ensure that there are no personal data breaches.
- 18.2. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.
- 18.3. Where appropriate, we will report the data breach to the ICO within 72 hours.

19. Training

- 19.1. All employees and governors are provided with data protection training as part of their induction process and will carry out annual refresh training.
- 19.2. Data protection will also form part of continuing professional development, where changes to legislation, guidance or our trust's processes make it necessary.

20. Monitoring arrangements

- 20.1. Our trust data lead is responsible for monitoring and reviewing this policy.
- 20.2. This policy will be reviewed annually and approved by our Trust Board.

21. Appendix 1

21.1. Personal Data Breach Procedure

- 21.1.1. This procedure is based on guidance on personal data breaches produced by the ICO.
- 21.1.2. On finding or causing a breach, or potential breach, the employee or data processor must immediately notify the DPO by email or phone.
- 21.1.3. The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - 21.1.3.1. lost.
 - 21.1.3.2. stolen.
 - 21.1.3.3. destroyed.
 - 21.1.3.4. altered.
 - 21.1.3.5. disclosed or made available where it should not have been.
 - 21.1.3.6. made available to unauthorised people.
- 21.1.4. If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the CEO, headteacher and chair of governors.
- 21.1.5. Employees and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- 21.1.6. The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant employees or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers) (see the actions relevant to specific data types at the end of this procedure).
- 21.1.7. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences.
- 21.1.8. The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool.
- 21.1.9. The DPO will document the decisions (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the GDPRiS online system
- 21.1.10. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
 - 21.1.10.1. a description of the nature of the personal data breach including, where possible:
 - 21.1.10.1.1. the categories and approximate number of individuals concerned.
 - 21.1.10.1.2. the categories and approximate number of personal data records concerned.
 - 21.1.10.1.3. the name and contact details of the DPO.
 - 21.1.10.1.4. a description of the likely consequences of the personal data breach.
 - 21.1.10.1.5. a description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- 21.1.11. If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- 21.1.12. Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
 - 21.1.12.1. a description, in clear and plain language, of the nature of the personal data breach.
 - 21.1.12.2. the name and contact details of the DPO.
 - 21.1.12.3. a description of the likely consequences of the personal data breach.
 - 21.1.12.4. a description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

- 21.1.13. The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- 21.1.14. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
- 21.1.14.1. facts and cause.
 - 21.1.14.2. effects.
 - 21.1.14.3. action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).
 - 21.1.14.4. records of all breaches will be stored the GDPRiS online system.
- 21.1.15. The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.
- 21.1.16. The DPO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

21.2. Example actions to minimise the impact of data breaches

- 21.2.1. We will take the actions set out below to mitigate the impact of different types of data breach. We will review the effectiveness of these actions and amend them as necessary after any data breach:
- 21.2.1.1. Investigate school systems to confirm the source of the breach.
 - 21.2.1.2. Interview employees and pupils to investigate the reason for the breach (e.g. malicious or accidental)
 - 21.2.1.3. Contact recipients of data and request that the data in question is deleted, and not shared, published or replicated, and evidence of this action is provided (e.g. screenshot of deletion)
 - 21.2.1.4. Attempt to remotely wipe a lost or stolen school phone or other device
 - 21.2.1.5. Log requests with internet-based providers to remove copies of any breached data.
 - 21.2.1.6. Change login credentials for any compromised accounts
 - 21.2.1.7. Document actions and outcomes

22. Appendix 2

22.1. Appropriate Policy Document

- 22.1.1. Processing of special categories of personal data and criminal offence data.
- 22.1.2. As part of our trust's functions, we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

22.2. Special category data

- 22.2.1. Special category data is defined at Article 9 UK GDPR as personal data revealing:
 - 22.2.1.1. racial or ethnic origin.
 - 22.2.1.2. political opinions.
 - 22.2.1.3. religious or philosophical beliefs.
 - 22.2.1.4. trade union membership.
 - 22.2.1.5. genetic data.
 - 22.2.1.6. biometric data for the purpose of uniquely identifying a natural person.
 - 22.2.1.7. data concerning health.
 - 22.2.1.8. data concerning a natural person's sex life or sexual orientation.

22.3. Criminal Conviction Data

- 22.3.1. Article 10 UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

22.4. This policy document

- 22.4.1. Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.
- 22.4.2. This document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.
- 22.4.3. In addition, it provides some further information about our processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements our privacy notices which are available on our trust website at [Mercia Learning Trust - Statutory Documentation \(merciatrust.co.uk\)](https://merciatrust.co.uk/Mercia-Learning-Trust-Statutory-Documentation)

22.5. Conditions for processing special category and criminal offence data

- 22.5.1. We process special categories of personal data under the following UK GDPR Articles:
 - 22.5.1.1. Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on our trust or the data subject in connection with **employment**, social security or social protection. Examples include our processing of employee sickness absences.
 - 22.5.1.2. Article 9(2)(g) - reasons of **substantial public interest**. Our trust is a public body. We are required by law to provide the UK Government with data that would count as special category data and are required by law to provide it. Our processing of personal data in this context is therefore necessary for the carrying out of our role.
 - 22.5.1.3. We are required by law to safeguard the pupils who attend our school and as such, some special category data will be processed to provide them with the appropriate support they need. Examples of our processing are support for individuals with a particular disability or medical condition, counselling and safeguarding of children and individuals at risk.
 - 22.5.1.4. Article 9(2)(j) – for **research** purposes in the public interest. The relevant purpose we rely on is Schedule 1 Part 1 paragraph 4 – research. An example of our processing is working with universities and the Department of Education to provide data for research purposes to help improve UK schools and education.
 - 22.5.1.5. Article 9(2)(h) – the treatment or the **management of health**. Examples include our processing of data received from an NHS professional or other healthcare worker about one of our pupils.
 - 22.5.1.6. Article 9(2)(i) – for reasons of public interest in the area of **public health**. Examples include our sharing data about our employees or pupils with the NHS in the case of a pandemic.

- 22.5.2. Article 9(2)(a) – **explicit consent**. In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing. Examples of our processing include information about pupil or employees dietary requirements, allergies and other health information that we require to look after the wellbeing of our pupils and workforce.
- 22.5.3. Where we use biometric data such as fingerprints for cashless catering, we rely on gaining explicit consent from the data subject or their parent/carer before using this data.
- 22.5.4. When we ask for ethnicity (requested by the DfE for school census returns) we make it clear that providing it is optional and by providing it the data subject (or their parent/carer) is consenting for it to be shared with the DfE.
- 22.5.5. Article 9(2)(c) – where processing is necessary to protect the **vital interests** of the data subject or of another natural person. An example of our processing would be using health information about a pupil or employee in a medical emergency.
- 22.5.6. We process criminal offence data under Article 10 of the UK GDPR. Examples of our processing of criminal offence data include pre-employment checks (DBS, barred list) and declarations by a member of our trust workforce in line with contractual or safeguarding obligations.

22.6. Processing which requires an Appropriate Policy Document

- 22.6.1. Almost all the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD (see Schedule 1 paragraphs 1 and 5).
- 22.6.2. This section of the policy is the APD for our trust. It demonstrates that the processing of special category ('SC') and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. In particular, it outlines our retention policies with respect to this data.

22.7. Description of data processed

- 22.7.1. Health and medical data - workforce and pupils.
- 22.7.2. Ethnicity - pupils and workforce.
- 22.7.3. Religion - pupils and workforce.
- 22.7.4. Biometric (fingerprint) data for cashless catering, access control or library systems.
- 22.7.5. Criminal records - DBS checks for all members of our trust workforce (paid and unpaid).
- 22.7.6. Further information about this processing can be found in our privacy notices.
- 22.7.7. We also maintain a record of our processing activities in accordance with Article 30 of the UK GDPR.

22.8. Schedule 1 Conditions for Processing

- 22.8.1. Special category data
- 22.8.2. We process SC data for the following purposes in Part 1 of Schedule 1:
 - 22.8.2.1. Paragraph 1(1) employment, social security and social protection.
- 22.8.3. We process SC data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:
 - 22.8.3.1. Paragraph 6(1) and (2)(a) Statutory and government purposes.
 - 22.8.3.2. Paragraph 8(1) and (2) Equality of opportunity or treatment.
 - 22.8.3.3. Paragraph 18(1) Safeguarding of children and of individuals at risk.
- 22.8.4. **Criminal offence data**
- 22.8.5. We process criminal offence data for the following purposes in parts 1 and 2 of Schedule 1:
 - 22.8.5.1. **Paragraph 1** – employment, social security and social protection

22.9. Procedures for Ensuring Compliance with the Principles

- 22.9.1. **Accountability principle**
 - 22.9.1.1. We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:
 - 22.9.1.1.1. the appointment of a data protection officer who reports directly to our highest management level.
 - 22.9.1.1.2. taking a 'data protection by design and default' approach to our activities.

- 22.9.1.1.3. maintaining documentation of our processing activities.
- 22.9.1.1.4. adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.
- 22.9.1.1.5. implementing appropriate security measures in relation to the personal data we process.
- 22.9.1.1.6. carrying out data protection impact assessments for our high-risk processing.

22.9.1.2. We regularly review our accountability measures and update or amend them when required.

22.9.2. Principle (a): lawfulness, fairness and transparency

- 22.9.2.1. Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.
- 22.9.2.2. We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice, employee privacy notice and this policy document.
- 22.9.2.3. Our processing for purposes of substantial public interest is necessary to function as a Trust under the Education Act 2005.
- 22.9.2.4. Our processing for the purposes of employment relates to our obligations as an employer.
- 22.9.2.5. We also process special category personal data to comply with other obligations imposed on our trust by the Department for Education or our local authority.

22.9.3. Principle (b): purpose limitation

- 22.9.3.1. We process personal data for the purposes explained above when the processing is necessary for us to fulfil our statutory functions as a Trust.
- 22.9.3.2. If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose.
- 22.9.3.3. We will not process personal data for purposes incompatible with the original purpose it was collected for.

22.9.4. Principle (c): data minimisation

- 22.9.4.1. We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

22.9.5. Principle (d): accuracy

- 22.9.5.1. Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

22.9.6. Principle (e): storage limitation

- 22.9.6.1. All special category data processed by us for the purpose of employment or substantial public interest is retained for the periods set out in our retention schedule.
- 22.9.6.2. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedule is reviewed regularly and updated when necessary.

22.9.7. Principle (f): integrity and confidentiality (security)

- 22.9.7.1. Electronic information is processed within our secure network. Paper copies of personal data are kept locked in filing cabinets in locked offices.
- 22.9.7.2. Our electronic systems and physical storage have appropriate access controls applied, only relevant employees have access to the files.
- 22.9.7.3. The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

22.10. Retention and Erasure Policies

- 22.10.1. Our retention and erasure practices are set out in our retention schedule which is available on request from our trust office.

22.11. APD review date

22.11.1. This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases. This policy will be reviewed annually or revised more frequently if necessary.

22.12. Additional special category processing

22.12.1. We process special category personal data in other instances where it is not a requirement to keep an appropriate policy document. Our processing of such data respects the rights and interests of the data subjects. We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice and workforce privacy notice.

