WESSEX
MULTI-ACADEMY TRUST

DATA PROTECTION POLICY

Adopted By:	**Board of Trustees**
Date:	**July 2025**
Review Date:	**July 2026**

DATA PROTECTION POLICY

Date of Issue:	July 2025
Policy applies to:	All staff/trustees/governors employed by the Wessex Multi-Academy Trust.
Policy Version Number:	3
Purpose of the document:	To provide an understanding of the policy and best practice for data protection
Summary of the main points:	This policy is in place to ensure all staff, trustees and governors are aware of their responsibilities and outlines how the Trust complies with the core principles of the UK GDPR.
Approved by:	This policy has been approved by the Wessex MAT Board of Trustees
Reviewer:	Sophia Radford, Data Protection Officer
Summary of amendments:	1. Amendments to Legal Framework 2. Amendments to Para 2.1 regarding definition of special categories of personal data 3. Re-write of Para 3. 4. Re-write of Para 4 to clarify role of school data leads. 5. Re-write of Para 8.4 to clarify capability of a child to understand their rights. 6. Re-write of Para 21.2 ref CCTV 7. Addition of Para 25 ref biometric recognition systems 8. Addition of Para 26 ref AI
Next review due:	July 2026

Contents

Statement of intent

Wessex Multi-Academy Trust and its schools are required to keep and process certain information about staff members, pupils, their families, volunteers and external contractors in accordance with our legal obligations under data protection legislation.

We may, from time to time, be required to share personal information about staff or pupils with other organisations, mainly the LA, DfE, other schools and educational bodies, and potentially children's services.

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

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

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Information sharing advice for safeguarding practitioners March 2015
- Protection of Freedoms Act 2012

- This policy also has regard to the following guidance:
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2012) 'IT asset disposal for organisations'
- DfE (2018) 'Data protection: a toolkit for schools'

- This policy operates in conjunction with the following school policies:
- Photography Policy
- Data and Cyber-security Breach Prevention and Management Plan
- Freedom of Information Policy
- Freedom of Information Publication Scheme
- Surveillance and CCTV Policy
- Child Protection and Safeguarding Policy
- Records Management 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 UK 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. **'Sensitive personal data'** is referred to in the UK GDPR as 'special categories of personal data', and includes information about an individuals:

- Genetic data.
- Biometric data (such as fingerprints where used for identification purposes).
- Data concerning health-physical or mental.
- Sex life or sexual orientation

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.

'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.

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:

- 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.

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 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 UK 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. Accountability

3.1. The Trust will seek to implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR, and provide comprehensive, clear and transparent privacy policies.

3.2. The Trust will seek to ensure each individual school within the Trust is adhering to the same procedure and that this is being implemented and enforced in line with the wider Trust policies.

3.3. The Trust/school will also document other aspects of compliance with the UK GDPR and DPA and will implement measures that meet the principles of data protection by design and data protection by default.

3.4. DPIAs will be used to identify and reduce data protection risks, where appropriate.

4. Data protection officer (DPO)/Data Protection Lead

4.1. The Trust is required to appoint a DPO who will be the central point of contact for all data subjects and others in relation to matters of data protection. In addition each school will appoint a Data Protection Lead to assist in promoting a culture of privacy awareness throughout the school community.

4.2. An existing employee will be appointed to the role of Data Protection Lead provided that their duties are compatible with the duties of the Data Protection Lead and do not lead to a conflict of interests.

4.3. The DPO will operate independently and will not be dismissed or penalised for performing their duties. Sufficient resources and appropriate access will be provided to the DPO to enable them to meet their UK GDPR obligations.

4.4. The DPO will report to the highest level of management at the Trust, which is the Board of Trustees.

4.5. Staff will ensure that they involve the Data Lead and/or DPO in all data protection matters closely and in a timely manner.

5. Lawful processing

5.1. The legal basis for processing data will be identified and documented prior to data being processed. 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 a contract held with the individual, or because they have asked the school to take specific steps before entering into a contract
- Processing is necessary for compliance with a legal obligation (not including contractual obligations)

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for protecting vital interests of a data subject or another person, i.e. to protect someone's life
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject – this condition is not available to processing undertaken by the Trust/school in the performance of its tasks

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

- Explicit consent of the data subject
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- 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 with a basis in 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 with a basis in law
  - 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 a basis in law
- When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data.

5.3. For personal data to be processed fairly, data subjects must be made aware:

- That the personal data is being processed.
- Why the personal data is being processed.
- What the lawful basis is for that processing.

- Whether the personal data will be shared, and if so, with whom.
- The existence of the data subject's rights in relation to the processing of that personal data.
- The right of the data subject to raise a complaint with the ICO in relation to any processing.

5.4. The Trust has privacy notices for the following groups, which outline the information above that is specific to them:

- Prospective employees
- Pupils and their families
- School workforce
- Third parties
- Trustees and governors
- Volunteers

5.5. There may be circumstances where it is considered necessary to process personal data or special category personal data in order 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.

5.6. Where the Trust/school relies on:

- 'Performance of contract' to process a child's data, the Trust/school considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a child's data, the Trust/school takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place.
- Consent to process a child's data, the Trust/school ensures that the requirements outlined in the 'Consent' section are met, and the Trust/school does not exploit any imbalance of power in the relationship between the Trust/school and the child.

6. Consent

6.1. Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told.

6.2. The Trust/school ensures that consent mechanisms meet the standards of the UK 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. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

6.3. When pupils and staff join the Trust/school, the staff member or pupil (or, where appropriate, pupil's parent) will be required to complete a consent form for personal data use. This consent form deals with the taking and use of photographs and videos, amongst other things. Where appropriate, third parties may also be required to compete a consent form.

6.4. Where the Trust/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 above, the Trust/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. 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, taking into account the requirements outlined above.

7. The right to be informed

7.1. Adults and children have the same right to be informed about how the Trust uses their data. The privacy notices supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language which is concise, transparent, easily accessible and free of charge.

7.2. 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, the controller's representative, where applicable, and the DPO
- The purpose of, and the lawful 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. The right of access

8.1. Individuals, including children, have the right to obtain a copy of their personal data as well as other supplementary information, including confirmation that their data is being processed, and the right to submit a data subject access request (DSAR) to gain access to their personal data in order to verify the lawfulness of the processing. The Trust/school will verify the identity of the person making the request before any

information is supplied.

8.2. A copy of the information will be supplied to the individual free of charge; however, the Trust/school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

8.3. Where a DSAR has been made electronically, the information will be provided in a commonly used electronic format.

8.4. Where a DSAR has been made for information held about a child, the Trust/school will evaluate whether the child is capable of fully understanding their rights. Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a DSAR. Therefore, most DSAR from parents or carers of pupils at primary and middle schools may 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. If the Trust/school determines the child is mature enough to understand their rights and the implications of a DSAR, it will respond directly to the child.

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

8.6. Where a request is manifestly unfounded or excessive, we hold 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.

8.7. We will seek to ensure that information released in response to a DSAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data, we will:

- Omit certain elements from the response if another individual's personal data would be disclosed otherwise.
- Reject requests that cannot be fulfilled without disclosing another individual's personal data, unless that individual consents or it is reasonable to comply without consent.
- Explain to the individual who made the SAR why their request could not be responded to in full.

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

relation to – the time limit for responding to the request will be paused until clarification from the individual is received.

9. The right to rectification

9.1. Individuals, including children, are entitled to have any inaccurate or incomplete personal data rectified.

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

9.3. Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, the Trust/school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once. We reserve the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

9.4. The Trust/school will take reasonable steps to ensure that data is accurate or is rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data. We will restrict processing of the data in question whilst its accuracy is being verified, where possible.

9.5. Where the personal data in question has been disclosed to third parties, the Trust/school will inform them of the rectification where possible. Where appropriate, we will inform the individual about the third parties that the data has been disclosed to.

9.6. Where no action is being taken in response to a request for rectification, or where the request has been investigated and the data has been found to be accurate, the Trust/school 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.

10. The right to erasure

10.1. Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals, including children, 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 or processed
- When the individual withdraws their consent where consent was the lawful basis on which the processing of the data relied
- 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

10.2. The Trust/school will comply with the request for erasure without undue delay and at the latest within one month of receipt of the request.

10.3. We have 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 establishment, exercise or defence of legal claims

10.4. The Trust/school has the right to refuse a request for erasure for special category data where processing is necessary for:

- Public health purposes in the public interest, e.g. protecting against serious cross-border threats to health.
- Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.

10.5. Requests for erasure will be handled free of charge; however, the Trust/school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

10.6. 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.

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

11. The right to restrict processing

11.1. Individuals, including children, have the right to block or suppress the Trust/school's processing of personal data.

11.2. We 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 we have verified the accuracy of the data
- Where an individual has objected to the processing and the school 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/school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

11.3. In the event that processing is restricted, the Trust/school 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. We will inform individuals when a restriction on processing has been lifted.

11.4. Where the Trust/school is restricting the processing of personal data in response to a request, it will make that data inaccessible to others, where possible, e.g. by temporarily moving the data to another processing system or unpublishing published data from a website.

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

11.6. We reserve the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. 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.

12. The right to data portability

12.1. Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies in the following cases:

- Where personal data has been provided directly by an individual 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

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

will be provided in a structured, commonly used and machine-readable form. Where feasible, data will be transmitted directly to another organisation at the request of the individual. The Trust/school will not be required to adopt or maintain processing systems which are technically compatible with other organisations.

12.3. The Trust/school will provide the information free of charge.

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

12.5. We will respond to any requests for portability within one month. 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.

12.6. Where no action is being taken in response to a request, the Trust/school 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.

13. The right to object

13.1. The Trust/school will inform individuals, including children, 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. Individuals, including children, have the right to object to the following:

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

13.2. 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/school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- The Trust/school will respond to objections proportionally, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress.

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

- The right to object is absolute and the Trust/school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Trust/school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- The Trust/school will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.

13.4. 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/school is not required to comply with an objection to the processing of the data.

13.5. Where the processing activity is outlined above, but is carried out online, the Trust/school will offer a method for individuals to object online.

13.6. The Trust/school will respond to all objections without undue delay and within one month of receiving the objection; this may be extended by a further two months if the request is complex or repetitive.

13.7. Where no action is being taken in response to an objection, the Trust/school 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. Automated decision making and profiling

14.1. The Trust/school will only ever conduct solely automated decision making with legal or similarly significant effects is the decision is:

- Necessary for entering into or performance of a contract.
- Authorised by law.
- Based on the individual's explicit consent.

14.2. Automated decisions will not concern a child nor use special category personal data, unless:

- The Trust/school has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest.

14.3. The Trust/school will conduct a DPIA for automated decision making to mitigate risk of errors, bias and discrimination.

14.4. The Trust/school will ensure that individuals concerned are given specific information about the processing and an opportunity to challenge or request a review of the decision.

14.5. Individuals have the right not to be subject to a decision when both of the following conditions are met:

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

14.6. The Trust/school 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.

14.7. When automatically processing personal data for profiling purposes, the Trust/school 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. Data protection by design and default

15.1. The Trust/school will act in accordance with the UK GDPR by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how we have considered and integrated data protection into all aspects of processing activities. In line with the data protection by default approach, we will ensure that only data that is necessary to achieve its specific purpose will be processed.

15.2. The Trust/school will implement a data protection by design and default approach by using a number of methods, including, but not limited to:

- Considering data protection issues as part of the design and implementation of systems, services and practices.
- Making data protection an essential component of the core functionality of processing systems and services.
- Automatically protecting personal data in Trust/school's ICT systems.

- Implementing basic technical measures within our network and ICT systems to ensure data is kept secure.
- Promoting the identity of the DPO as a point of contact.
- Ensuring that documents are written in plain language so individuals can easily understand what is being done with personal data.

16. Data Protection Impact Assessments (DPIAs)

16.1. DPIAs will be used in certain circumstances to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow the Trust and its schools to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to our reputation which might otherwise occur. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals, and will be used for more than one project, where necessary.

16.2. 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

16.3. The Trust and its schools 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

16.4. Where a DPIA indicates high risk data processing, the Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

17. Data breaches

17.1. 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. The Trust will provide training to Data Leads to ensure that all staff are made aware of, and understand, what constitutes a data breach as part of their training.

17.2. The Trust provides guidance on investigation and access to internal reporting procedures to facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

17.3. Where the Trust/school faces a data security incident, the DPO will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it.

17.4. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the Trust or its schools becoming aware of it. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed, and the individuals concerned will be contacted directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. 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. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

17.5. Within a breach notification to the supervisory authority, 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

17.6. Where notifying an individual about a breach to their personal data, the Trust/school will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.

17.7. The Trust/school will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the UK GDPR accountability principle and in accordance with the Records Management Policy.

17.8. The Trust/school will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by mandating data protection refresher training where the breach was a result of human error.

18. Data security

18.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access, and will not be left unattended or in clear view anywhere with general access.

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

data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use. Use of external media is not supported. All electronic devices are password-protected to protect the information on the device in case of theft. At present all central team electronic devices enable remote blocking or deletion of data in case of theft.

18.3. If staff, trustees or governors need to use their personal devices for Trust/school purposes, particularly if they are working from home, they will ensure that the device has the latest security patches and anti-malware updates installed. In school they will use a separate Guest Wifi SSID, ensuring no connection to the school internal network. Where personal devices are used these are only used with the express consent of the Trust and staff, trustees or governors must not use personal devices to capture and/or store documents and images on personal devices.

18.4. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient. When sending confidential information staff must always check that the recipient is correct before sending.

18.5. Before sharing data, all staff must 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.

18.6. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff must 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 school premises accepts full responsibility for the security of the data.

18.7. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Trust and its schools containing sensitive information must be supervised at all times.

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

18.9. Each school's Data Protection Lead is responsible for data protection within their setting and will use their best endeavours to ensure continuity and recovery measures are in place to ensure the security of protected data.

18.10. When disposing of data, paper documents will be shredded and digital storage devices will be physically destroyed when they are no longer required; all ICT assets will be disposed of by a certified IT asset disposal company and a certificate will be received for the data destruction in accordance with the ICO's guidance on the disposal of ICT assets.

Commented [SR1]: Confirm with Oakford re disposal of ICT assets

Commented [KW2R1]: Addition from Olli

18.11. The Trust holds the right to take the necessary disciplinary action against a staff member if they believe them to be in breach of the above security measures.

19. Safeguarding

19.1. We will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the school's DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

19.2. The Trust and its schools will aim to gain consent to share information where appropriate; however, we will not endeavour to gain consent or share information if to do so would place a child at risk. We will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

20. Publication of information

20.1. The Trust publishes a Freedom of Information Publication Scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Organisational information
- Strategy and performance information
- Financial information

20.2. Classes of information specified in the Freedom of Information Publication Scheme are made available quickly and easily on request.

21. CCTV and photography

21.1. The Trust and its schools understand that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

21.2. The Trust and its schools may use CCTV in various locations around our sites to ensure the site remains safe. The Trust/ schools will adhere to the ICO code of practice for the use of CCTV. The Trust/ schools do not need to ask individuals'

permission to use CCTV, but will make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. The Trust/schools will notify all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email. Cameras are only placed where necessary to fulfil their purpose. All CCTV footage may be kept for 30 days for security purposes; each school is responsible for keeping the records secure and allowing access.

21.3. The Trust will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them. If the Trust/school wishes to use images or video footage of pupils in a publication, such as a website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

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

21.5. Parents and others attending Trust or school events are able to take photographs and videos of those events as long as they are for domestic purposes only and are not shared. Photographs or videos being used for any other purpose are prohibited to be taken by parents or visitors. The Trust or school may request that photographs and videos are not taken if this may cause any safeguarding concerns.

21.6. The Trust and its schools asks that parents and others do not post any images or videos which include any children other than their own on any social media or otherwise publish those images or videos.

22. Cloud computing

Commented [SR3]: Review this clause with Oakford.

Commented [KW4R3]: See below

22.1. For the purposes of this policy, **'cloud computing'** refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the Trust and its schools accessing a shared pool of ICT services remotely via a private cloud environment. Files are only accessible from a school device and/or a school location. Files are accessed directly and not copied or downloaded for use.

22.2. All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

22.3. If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the Trust. Multifactor Authentication (MFA) will be enabled for cloud services where possible.

22.4. All files and personal data placed in the cloud will be subject to robust security measures at all times, including when the data is 'in transit' between the device and cloud. The Trust will review its use of cloud computing with ICT to ensure ongoing

compliance and security of data.

22.5. As with files on devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the Trust/school should unauthorised access, deletion or modification occur and ensure ongoing compliance with our policies for the use of cloud computing.

22.6. The Trust/school's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by with the support of the school's IT provider.

Commented [SR5]: Remove and include Oakford contact details.

23. Data retention

23.1. Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable. Some educational records relating to former pupils or employees of an school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts. Paper documents will be shredded or pulped. Electronic memories will be securely disposed of.

24. DBS data

24.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. 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. Biometric recognition systems

25.1 Schools may use pupils' biometric data as part of an automated biometric recognition system. Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

25.2 Parents/carers and pupils have the right to choose not to use the school's biometric system(s). 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)/carer(s).

25.3 Where staff members 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. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

26. Artificial Intelligence

26.1.1 The Trust acknowledges that artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The Trust recognises that AI has many uses to help

pupils learn but also poses risks to sensitive and personal data. To ensure that personal and sensitive data remains secure, the Trust/ schools will ensure that all users are aware that they will not be permitted to enter such data into unauthorised generative AI tools or chatbots. If personal and/or sensitive data is entered into an unauthorised generative AI tool, the Trust/ schools will treat this as a data breach, and will follow the personal data breach procedure.

27. Monitoring and review

27.1. This policy is reviewed annually by the DPO. The next scheduled review date for this policy is July 2026.