Horizons Specialist Academy Trust
Providing infinite opportunities

Horizons Specialist Academy Trust

Data Protection Policy

Adopted by the Board of Trustees: 29 September 2021
Date of next review: Autumn term 2023
Responsible Officer: Data Protection Officer

Contents: Page

Statement of intent

Horizons Specialist Academy Trust ("the Trust") is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the UK General Data Protection Regulation (GDPR).

The Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly relevant LAs, other schools and educational bodies, and potentially children's services.

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 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.

Public Sector Equality Duty

Horizons Specialist Academy Trust has carefully considered and analysed the impact of this policy on equality and the possible implications for pupils, parents and staff with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

1. Legal framework

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

- The UK General Data Protection Regulation (GDPR)
- The Data Protection Act (2018)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- Protection of Freedoms Act

1.2. This policy will also have regard to the following guidance:

- Information Commissioner's Office (ICO) (2021) 'Guide to the UK General Protection Regulation (GDPR)'
- DfE (2018) 'Data Protection: a toolkit for schools'
- Information Commissioner's Office (ICO)(2021) 'IT asset disposal organisations'

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

- Photography and Video Policy
- E-security Policy
- Information Security Policy
- Freedom of Information Policy
- CCTV Policy
- Records Management Policy
- Child Protection Policy

2. Applicable data

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

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

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

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

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

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 in connection with employment, social security, social protection, health or social care purposes, public health and research.

3. Principles

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

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

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

4. Accountability

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

4.2. The Trust will provide comprehensive, clear and transparent privacy policies.

4.3. Additional internal records of the Trust's processing activities will be maintained and kept up-to-date.

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

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

4.5. The Trust will also document other aspects of compliance with the UK GDPR and Data Protection Act (2018) where this is deemed appropriate in certain circumstances by the DPO, including the following:

- Information required for privacy notices, e.g. the lawful basis for processing
- Records of consent
- Controller-processor contracts
- The location of personal data
- Data Protection Impact Assessments (DPIA)
- Records of personal data breaches

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

- Minimising the processing of personal data.
- Pseudonymising personal data as soon as possible.
- Ensuring transparency in respect of the functions and processing of personal data
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

4.7. DPIAs will be used, where appropriate.

5. Data protection officer (DPO)

5.1. A DPO will be appointed in order to:

- Inform and advise the Trust and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the Trust's compliance with the GDPR and other applicable laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.
- Co-operate with the ICO and act as the first point of contact for the ICO and for individuals whose data is being processed.

5.2. The DPO is responsible for:

- Co-ordinating a proactive and preventative approach to data protection
- Calculating and evaluating the risks associated with the Trust's data processing
- Having regard to the nature, scope, context and purpose of all data processing
- Prioritising and focussing on ore risky activities, e.g. where special category data is being processed
- Promoting a culture of privacy awareness throughout the Trust community
- Carrying out ad hoc reviews of data protection to ensure staff understand and are acting in accordance with relevant Data Protection laws

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

5.4. The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

5.5. The DPO will report to the highest level of management, which is the Chief Executive (CEO).

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

5.7. Staff will ensure that they involve the DPO in all data protection matters closely and in a timely manner.

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

6. Lawful processing

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

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

- The consent of the data subject has been obtained.
- Processing is necessary for:
  - Compliance with a legal obligation (processing undertaken by the Trust in the performance of its tasks)
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - For the performance of a contract with the data subject or to take steps to enter into a contract.
  - Protecting the vital interests of a data subject or another person.
  - For the purposes of legitimate interests pursued by the controller or a third party, except 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 in the performance of its tasks)

6.3. 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
- There may be circumstances where it is considered necessary to process personal data or special category 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.

6.4. Where the Trust relies on:

- 'Performance of contract' to process a child's data, the Trust 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 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 ensures that the requirements outlined in 7.7 and 7.8 are met, and the Trust does not exploit any imbalance of power in the relationship between the Trust and the child.

7. Consent

7.1. Consent must be a positive indication. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes.

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

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

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

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

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

7.7. Where online services are provided directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined in 7.2, consent should be obtained 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. The ICO has confirmed that this only applies if the service is provided *directly* to a child, and not through an intermediate such as a school.

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

8. Sharing data without consent

8.1 The Trust may share information without consent in specific circumstances. To determine whether information can be shared without consent, the Trust will identify one of the other lawful bases for processing:

- **Contract** – the processing is necessary for a contract held between the Trust and individual.
- **Legal obligation** – the processing is necessary for the Trust to comply with the law (not including contractual obligations).
- **Vital interests** – the processing is necessary to protect someone's life.
- **Public task** – the processing is necessary for the Trust to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.
- **Legitimate interests** – the processing is necessary for the Trust's legitimate interests or the legitimate interests of a third party, unless there is good reason to protect the individual's personal data which overrides those legitimate interests.

8.2 Where the Trust is able to justify one of the lawful bases outlined in 8.1, an exemption applies, or there is a requirement under another law, information may be shared without consent.

8.3 Specifically, the GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe, and information may be shared without consent if to gain consent would place a child at risk.

9. The right to be informed

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

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

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

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

9.4. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

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

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

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

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

10. The right of access

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

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

10.3. Where a SAR has been made for information held about a child, the Trust will evaluate whether the child is capable of fully understanding their rights. If the Trust determines the child can understand their rights, it will respond directly to the child.

10.4. The Trust will verify the identity of the person making the request before any information is supplied.

10.5. A copy of the information will be supplied to the individual free of charge; however, the Trust 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.

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

10.7. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

10.8. All fees will be based on the administrative cost of providing the information.

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

10.10. 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.

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

10.12. The Trust will ensure that information released in response to a SAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data the Trust 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

10.13. In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to – the time limit for responding to the request will be paused until clarification from the individual is received.

11. The right to rectification

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

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

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

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

11.5. Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, the Trust may impose a 'reasonable fee' to cover the administration costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

11.6. The Trust will restrict processing of the data in question whilst its accuracy is being verified, if possible.

11.7. The Trust reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

11.8. 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 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.

12. The right to erasure

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

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

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

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

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

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.

- For archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- The establishment, exercise or defence of legal claims.

12.5. The Trust 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 of social care, or the management of health or social care systems or services.

12.6. Requests for erasure will be handled free of charge; however the Trust 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.

12.7. 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.

12.8. 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.

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

13. The right to restrict processing

13.1. Individuals have the right to block or suppress the Trust's processing of personal data.

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

13.3. The Trust will restrict the processing of personal data in the following circumstances:

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

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

13.5. Where the Trust 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.

13.6. The Trust will inform individuals when a restriction on processing has been lifted.

13.7. The Trust reserves 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 refusal.

14. The right to data portability

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

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

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

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

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

14.5. The Trust will provide the information free of charge.

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

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

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

14.9. The Trust will respond to any requests for portability within one month.

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

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

15. The right to object

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

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

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

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

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

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

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

15.5. Where personal data is processed for research purposes:

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

15.6. The DPO will ensure that details are recorded for all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings.

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

15.8. The Trust 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.

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

16. Automated decision making and profiling

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

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

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

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

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

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

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

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

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

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

17. Privacy by design and default

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

17.2. In line with the data protection by default approach, the Trust will ensure that only data that is necessary to achieve its specific purpose will be processed.

17.3. The Trust 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 cure functionality of processing systems and services
- Automatically protecting personal data in the Trust ICT system
- 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.

18. Data Protection Impact Assessments (DPIAs)

18.1. 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.

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

18.3. 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.

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

18.5. 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.

18.6. The Trust will ensure that all DPIAs include the following information:
- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

18.7. Where a DPIA indicates high risk data processing, the Trust will consult the Information Commissioner's Office (ICO) to seek its opinion as to whether the processing operation complies with the GDPR.

19. Data breaches

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

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

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

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

19.5. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the Trust becoming aware of it.

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

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

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

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

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

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

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

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

19.13. The Trust 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 GDPR accountability principle.

19.14. The Trust will work to identify the cause of the breach and assess how a recurrence can be prevented.

20. Data security

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

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

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

20.4. Where 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.

20.5. Memory sticks will not be used to hold personal information unless permission has been obtained, they are password-protected and fully encrypted.

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

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

20.8. Staff will not use their personal laptops or computers for Trust purposes when personal data is being used.

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

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

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

20.12. When sending confidential information by fax, staff will always check that the recipient is correct before sending.

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

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

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

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

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

20.17. The Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

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

21. Safeguarding

21.1. The Trust understands that the GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

21.2. The Trust 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 reasonable possible.

21.3. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the Designated Safeguarding Lead will ensure 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 reasons that consent has not been sought, where appropriate
- If data was not share, state the reason

21.4. The Trust will aim to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk.

21.5. The Trust will manage all instances of data sharing for the purpose of keeping a child safe in line with the Child Protection Policy.

22. Publication of information

22.1. The Trust publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information

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

22.3. The Trust will not publish any personal information, including photos, on its websites without the permission of the affected individual.

22.4. When uploading information to the Trust's websites, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

23. CCTV and photography

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

23.2. The Trust notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

23.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

23.4. Retention of CCTV footage is detailed in the CCTV Policy, reflecting individual academy systems. Named individuals identified in the CCTV Policy are responsible for keeping the records secure and allowing access.

23.5. The Trust will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

23.6. If the Trust wishes to use images/video footage of pupils in a publication, such as the Trust's websites, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

23.7. Precautions, as outlined in the Photography and Video Policy, are taken when publishing photographs of pupils, in print, video or on the Trust's websites.

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

24. Biometric data

21.1 Where the Trust uses pupils' biometric data as part of an automated biometric recognition system (e.g. fingerprints to access school dinners instead of paying cash), the Trust will comply with the requirements of the Protection of Freedoms Act 2012.

21.2 Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Trust will seek written consent from at least one parent or carer before we take any biometric data from their child and first process it.

21.3 Parents/carers and pupils have the right to choose not to use biometric systems. If a biometric system is introduced, the Trust will provide alternative means of accessing the relevant services for those pupils.

21.4 Parents/carers and pupils can object to participation in a biometric system or withdraw consent at any time, and the Trust will make sure that any relevant data already captured is deleted.

21.5 As required by law, if a pupil deemed to have capacity to make decisions, 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).

21.6 Where staff members or other adults use the biometric system(s), the Trust 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 Trust will ensure any relevant data already captured is deleted.

25. Taking personal data home

22.1 The GDPR does not prevent staff taking personal data home to work on.

22.2 Documents with little personal data, such as student work books or coursework, are essentially low risk as they contain minimal personal data.

22.3 There are also documents with more substantial amounts of information, ie EHCPs, annual/termly reports, etc. that contain more substantial amounts of personal data.

22.4 If staff are removing documents to work on at home these must be kept securely, ie be kept somewhere specific at home that is not accessible by anyone else, not left in cars etc. It is the responsibility of anyone taking personal data home to ensure that security of the data is paramount. Failure to do this could result in a data breach (see section 19 above).

26. Data retention

26.1. Data will not be kept for longer than is necessary.

26.2. Unrequired data will be deleted as soon as practicable.

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

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

27. DBS data

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

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

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

28. Policy review

28.1. This policy is reviewed every two years by the DPO.

28.2. The next scheduled review date for this policy is the autumn term 2023.