Epworth Education Trust

General Data Protection Regulations (GDPR) Policy

EPWORTH

EDUCATION TRUST

Written by:	J Buckley, Trust Business Manager
Date agreed:	Oct 2021
Next Review Date:	Autumn 2022
Chairs Signature	

Contents:

Statement of intent

The Epworth Trust is required to keep and process certain information about its staff members, pupils, their families, volunteers, extended contractors and pupils in accordance with its legal obligations under the Data Protection legislation.

The Epworth Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, 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 school complies with the following core principles of the UK GDPR.

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

Please note: This policy has been updated following Brexit and the adopting of the GDPR into UK law as the UK GDPR.

Although schools must now have regard to the UK GDPR instead, there have been no significant changes to the content of the legislation beyond minor technical changes to ensure that it can function in a UK-only context.

1. Legal framework

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

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

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

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- DFE Guidance on cloud software services and the DFA
- DFE Guidance on Information Sharing

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

- Use of images and Photography Policy
- E-security Policy
- Freedom of Information Policy
- CCTV Policy
- Confidentiality Policy
- Social Media Policy
- Online Safety Policy

1.4 This policy applies to all the schools within the Epworth Trust and the services it provides (Startwell Centre, Mighty Oaks).

Epworth Trust (Trust) – the academy trust that includes Westleigh Methodist (WLM) and Bedford Hall Methodist (BHM), the Westleigh Startwell Centre and it's hubs and its before and after school club (Mighty Oaks).

2. Definitions

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Company Personnel: all employees, workers [contractors, agency workers, consultants,] directors, volunteers, governors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. The UK GDPR applies to both automated personal data and to manual

filing systems, where personal data is accessinle according to specific criteria, as well as to chronologically ordered data and pseudonymised data e.g. key-coded.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or pupil privacy notices) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, data concerning health, data concerning a person's sex life, data concerning a person's sexual orientation.

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.

Senior Leadership Team (SLT): includes Headteachers, Deputy Manager, Startwell Manager, CEO, Trust Business Manager, HR and Facilities Manager and Assistant Head and B&A School club Managers.

3. Roles and Responsibilities

3.1. The Data Controller

3.1.1. The Epworth Trust, as the corporate body, is the data controller.

3.1.2. The Trustees of the Trust therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations and that the school is complying with its obligations under the UK General Data Protection Regulation.

3.1.3. The school SLT will deal with the day-to-day matters relating to data protection.

3.1.4. The SLT is responsible for ensuring personal information relating to pupils, staff, volunteers, governors and visitors is processed correctly by the relevant staff.

3.1.5. On occasion, personal information may be processed by outside organisations involved in data processing. By involving another organisation in data processing, the Trust increases certain risks. The security of the personal information is covered in a formal contract between the Trust / School and any outside organisation. See appendix 1 for an example of the formal contract used.

3.1.6. The SLT will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data. Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy.

3.1.7. All staff, trustees and governors will sign a privacy standard to acknowledge that they understand and will follow the procedures set by the school on how personal data is to be handled.

3.1.8. The Epworth Trust is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

3.2. The Data Protection Officer (DPO)

3.2.1. A DPO will be appointed in order to:

- Inform and advise the organisation / schools within 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 UK GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.
- Be the first point of contact with the ICO and data subjects

3.2.2. The DPO is responsible for :

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

3.2.3. The Trust must ensure that the appointed DPO's day to day duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

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

3.2.5. The DPO will report to the highest level of management at the Trust, which is the Board of Trustees via the Audit Committee

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

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

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

3.2.9. The Trust has appointed the following DPO:

- Joanne Buckley – Epworth Education Trust DPO

4. Principles

4.1. The Epworth Trust adhere to the Principles relating to Processing of Personal Data set out in the UK GDPR which requires personal data to 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 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.

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

5. Accountability

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

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

5.3. The Trust will be able to demonstrate how data is processed as a whole across the MAT, and will 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.

Additional internal records of the school's processing activities will be maintained and kept up-to-date. 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
- Storage locations

- Description of technical and organisational security measures
- Details of transfers to third parties, including documentation of the transfer mechanism safeguards in place

5.4. In order to create such records, data maps should be created which should include the details set out above together with appropriate data flows.

5.5. The school will also document other aspects of compliance with the UK GDPR and Data Protection Act where this is deemed appropriate in certain circumstance by the DPO, including the following:

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

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

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

6. Lawful processing

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

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

- The consent of the data subject has been obtained.
- Processing is necessary for:
  - Compliance with a legal obligation.
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - For the performance of a contract with the data subject or to take steps to enter into a contract.
  - Protecting the vital interests of a data subject or another person.
  - For the purposes of legitimate interests pursued by the controller or a third party, except 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 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 or a contract with a health professional.
  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law
- 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.

- 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.
- Where the school relies on:
    - 'Performance of contract' to process a child's data, the 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 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 school ensures that the requirements outlined in section 8 are met, and the school does not exploit any imbalance of power in the relationship between the school and the child.

7. Data Subject's Rights and Requests

7.1. Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw **Consent** to Processing at any time;
- **receive certain information** about the Data Controller's Processing activities;
- request **access** to their Personal Data that we hold;
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to **erase** Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to **rectify** inaccurate data or to complete incomplete data;
- **restrict** Processing in specific circumstances;
- **challenge** Processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- object to decisions based solely on **Automated Processing**, including profiling (ADM);
- prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority; and
- in limited circumstances, receive or ask for their Personal Data to be **transfer**red to a third party in a structured, commonly used and machine readable format.

7.2. Further information about these rights including the Epworth Trust procedures in dealing with these rights are detailed below. It is essential to verify the identity of an individual requesting data under any of the rights listed above (Personal data cannot be disclosed to third parties proper authorisation).

8. Consent

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

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

8.3. Consent may need to be refreshed if the use of the Personal Data is for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

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

8.5. The Trust 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.

8.6. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; Acceptable consent obtained under the DPA will not be reobtained.

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

8.8. When pupils and staff join the 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.

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

9. The right to be informed (Privacy Notices)

9.1. Adults and children have the same right to be informed about how the school 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.

9.2. 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 (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.

9.3. 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.

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

9.5. This information will be supplied:

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

9.6. Personal information is only made available to staff, trustees and governors who need that particular information to do their jobs, and is only made available at the time that it is needed.

10. The right of access

10.1. 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 subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. The school will verify the identity of the person making the request before any information is supplied.

10.2. 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. 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.

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

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

10.5. 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.

10.6. 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.

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

10.8. The school 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 school 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.

11. The right to rectification

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

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

11.3. Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, the 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. The school reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

11.4. The 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. The school will restrict processing of the data in question whilst its accuracy is being verified, where possible.

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

11.6. 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 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.

11.7. The accuracy of any personal data must be checked at the point of collection and at regular intervals afterwards. Measures must be taken to destroy or amended inaccurate or out of date personal data.

11.8. Members of staff and parents/carers are responsible for checking that any information that they provide to the Trust, in connection with their employment or in regard to a child, is accurate and up-to-date.

11.9. The Trust cannot be held accountable for any errors unless the employee or parent has informed the Trust about such changes.

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 to a child

12.3. The school 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 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.

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

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 school 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 school has 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 school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

13.4. Where the 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.

13.5. The school 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 the refusal.

13.6. 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.

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

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:

- Where 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. 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.

14.10. Where no action is being taken in response to a request, the 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.

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.
- The Trust 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.

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.
- The Trust will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.

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

15.7. 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. The 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.

15.8. Where no action is being taken in response to an objection, the 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.

16. Automated decision making and profiling

16.1. The Trust 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.

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

16.5. 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

16.6. 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.

16.7. 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. Data Protection by design and privacy impact assessments

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

protection by default approach, the school will ensure that only data that is necessary to achieve its specific purpose will be processed.

17.2. 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 core functionality of processing systems and services.
- Automatically protecting personal data in school ICT systems.
- Implementing basic technical measures within the school 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.

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

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

17.5. 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.

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

17.7. 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.

17.8. 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

17.9. 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 GDPR.

18. Data breaches

18.1. 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.

18.2. The SLT will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their induction/ refresher training.

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

18.4. **All breaches must be reported to the Trust DPO immediately**.

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

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

18.7. A ‘high risk’ breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

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

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

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

18.11. 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

18.12. Where notifying an individual about a breach to their personal data, the 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.

18.13. The 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.

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

18.15. The school with the DPO 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.

19. Data security and Confidentiality

19.1. The Trust will ensure data security is maintained by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
- Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

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

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

19.4. 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.

19.5. 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.

19.6. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

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

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

19.9. Where possible Staff, trustees and governors will not use their personal laptops or computers for school purposes.

19.10. All necessary members of staff are provided with their own secure login and password. They must update their password in line with the Trust Password policy

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

19.12. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients. In most circumstances, the school's parent mailing system will be used.

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

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

19.15. 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.

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

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

19.18. The School business manager or admin team with the Headteacher are responsible for continuity and recovery measures are in place to ensure the security of protected data.

19.19. 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.

19.20. The school will regularly test, assess and evaluate the effectiveness of any and all measures in place for data security.

19.21. When disposing of data, paper documents will be shredded and digital storage devices will be physically destroyed when they are no longer required. ICT assets will be disposed of in accordance with the ICO's guidance on the disposal of ICT assets.

19.22. 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.

20. Cloud Software Services

20.1. Responsibility for all areas of data protection compliance still rests with the Trust even when using cloud based software.

20.2. The key obligations that need to be addressed under UK GDPR are:

- Data Processing – The Trust must ensure a contract and data processing agreement is in place with the supplier to ensure they comply.
- Data Confidentiality – The supplier must provide to the Trust sufficient guarantees about the technical and organisational security measures governing the processing to be carried out.

- Data Integrity – Data integrity is defined as "the property that data is authentic and has not been maliciously or accidently altered during processing, storage or transmission" Suppliers need to confirm compliance
- Service Availability – There may be accidental loss of network connectivity between the Trust and the service provider. Therefore the Trust should ensure measures are in place to cope with the possibility of disruptions such as backup internet links (depending on level of risk)
- Use of Advertising – The Trust will not permit any cloud based software provider to engage in advertisement related data mining/profiling activities without their consent.

20.3. The Trust before subscribing and using any cloud based software will ensure its suppliers comply with the GDPR and its main provisions. This is carried out by asking the supplier to complete a self-certification checklist which the Department for Education is currently facilitating. In some cases the a Privacy Impact Assessment may be carried out (see DFE guidance on code of practise on PIAS

21. Publication of information

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

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

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

21.3. The Trust will not publish any personal information, including photos, on its website without the permission of the affected individual. When uploading information to the Trust/school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

22. CCTV and photography

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

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

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

22.4. All CCTV footage will be kept in accordance with the CCTV policy for security purposes; SLT are responsible for keeping the records secure and allowing access.

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

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

22.7. Precautions, as outlined in the Use of Images and Photography Policy, are taken when publishing photographs of children, in print, video or on the Trust website.

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

22.9. Parents and others attending school events are able to take photographs and videos of those events as long as they are for domestic purposes only. Photographs or videos being used for any other purpose are prohibited to be taken by parents or visitors to the school.

22.10. The school asks that parents and others do not post any images or videos which include any child other than their own child(ren) on any social media or otherwise publish those images or videos.

23. Data Retention

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

23.2. Unrequired data will be deleted as soon as practicable. This includes requiring third parties to delete such data where applicable.

23.3. The Trust will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

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

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

24. DBS Data

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

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

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

25. Training and Audit

25.1. All members of staff, including Trustees and Governors will receive training to enable them to comply with data privacy laws as part of their induction.

25.2. The training is reinforced at regular intervals throughout their employment or term as Governor and Trustee.

25.3. A regular review of all the systems and processes in place will take place to ensure compliance with UK GDPR and that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

26. Policy review

26.1. This policy is reviewed every year by the Date Protection Officer.

26.2. The next scheduled review date for this policy is May 2022.

Appendix 1

DATA PROCESSOR AGREEMENT

between The Epworth Trust and xxxxxxx

Under the Data Protection Act 1998, The Epworth Trust is required to put in place an agreement in writing with any organisation which processes personal data on its behalf to govern the processing of those data. This is to ensure anyone processing personal information on behalf of **The Trust** agrees to ensure the same level of security in respect of that information to ensure the Trust and its academies continue to meet their obligations under the Data Protection Act 1998.

Under a services agreement made between xxxxx and **xxxxx** on xxxxx ('the Agreement') xxxxx has agreed to provide a service to **The Trust** which requires xxxxx to have access to personal data for which **The Trust** is (and remains) the 'data controller' for the purposes of the GDPR. The other party to this agreement, xxxxx, will be a 'data processor' under that Act.

xxxxx agrees to store and process the personal data in accordance with the terms of this data processor agreement as set out below. The parties agree that the terms of this data processor agreement shall be incorporated and shall form part of the terms and conditions of the Agreement. To the extent that any of the terms of this data processor agreement conflict with the terms of the Agreement, the terms of this data processor agreement shall prevail.

1. Parties to the agreement:
The **Trust** and the **third party (xxxxx)**
2. Contacts
3. Service to be provided
Provide a brief re. the service to be provided
4. End date
The end date of this agreement will be xxxxx from the start date. The start date is the date this agreement is signed by xxxxx. Should The Trust agree to extend the contract for the provision of the xxxxx with xxxxx beyond 12 months from the start date, this agreement will also need to be renewed.
5. Personal data to be provided to XXXXXX
Insert the type of personal data that will be processed.
6. Transmission of personal data
If the personal data is being transmitted between parties, it must be clearly stated what means of transfer, ie. encrypted email, secure mailbox, encrypted file transfer.
7. Security of personal data
See notes re. security required
8. Retention of personal data
XXXXXXXXXXXX will securely retain **The Trust's** data until completion or termination of the contract.
9. Destruction of personal data

Upon completion or termination of the contract, all **The Trust** data must be returned to the **Trust** and then wiped from **XXXXXXXXXX** computer systems to British HMG Infosec Standard 5 (Enhanced Standard) levels or equivalent.

10. Subject access requests

The Trust has a process to manage Subject Access Requests and agrees to service where required, all subject access requests received. Any requests received in relation to information held by **the Trust** that has derived from this agreement will be dealt with under this process and will be responded to within 1 month..

11. Amending, transferring or deleting personal data

XXXXXXXXX must not amend any of **The Trust's** data. **XXXXXXXXX** must not transfer any of **The Trust's** data to any external or third party for any reason. **XXXXXXX** must not delete any of **The Trust** data other than at the end of the contract and in accordance with section 10 of this agreement.

12. Record-keeping and auditing compliance with this agreement

The trust will store a copy of this agreement. The Epworth **Trust** can at any time request and carry out a site visit to XXXXXXXXXX to audit compliance to the agreement. Or the **Epworth Trust** may request such documents, or any other material, from **XXXXXXXXXXXXXX** that will enable an audit of the agreement at any time.

13. Complaints

In the event of a complaint/allegation of misuse of personal information against **XXXXXXXXX**, the **trust** will seek and follow the advice from the Information Commissioner.

14. Breach of the data processor agreement

XXXXXXXXXX acknowledges and agrees that **The Epworth Trust** retain all rights, title and interest in the personal data subject to this agreement. **The Epworth Trust** remain the Data Controllers and are responsible for the processing carried out by **XXXXXXXXXXXXXXXXXX**.

On this basis, **XXXXXXXXXXXX** will fully indemnify **The Epworth Trust** in respect of any monetary penalty issued by the Information Commissioner's Office and any other claim, loss, liability or costs incurred arising as a result of a breach of this Agreement or as a result of any negligence or breach of statute or common law in processing the information disclosed to it.

15. Signatories

For **The Epworth Trust**:	For XXXXXXXXXXX:
Signed……	Signed……
Full name …….	Full name ……
……	……
Position……..	Position……..
……	……
Date……	Date……