EBOR ACADEMY TRUST

Policy Number

19

Data Protection Policy

Approved By:	Audit and Risk Committee
Approval Date:	June 2026
Review Period:	Every 2 years (subject to legislative/regulatory changes)
Review Date:	June 2028

Author: Wendy Harrington Head of Governance & Compliance
Date Created/updated: June 2026
Version Number: 5

Contents:

1. Policy Statement

1.1. Ebor Academy Trust aims to ensure that all staff, pupils, parents, governors, visitors and other individuals' personal data is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR), Data Use and Access Act 2025 and the Data Protection Act 2018 (DPA 2018). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

1.2. Compliance with the UK GDPR is described by this policy and other relevant policies such as the E-Safety Policy and the Acceptable Use Policy, along with connected processes and procedures.

1.3. This policy applies to all personal data processed by Ebor Academy Trust and its schools irrespective of the source.

1.4. Ebor Academy Trust is the data controller with responsibility for each of the Academies in the Trust. The Trust is responsible, with support from the schools for maintaining a record of processing activities updated as appropriate when those activities change. This record will be made available to the supervisory authority upon request.

1.5. This policy applies to all Employees/Staff of Ebor Academy Trust such as outsourced suppliers. Any breach of this policy may be dealt with under Trust's disciplinary policy and may also be a criminal offence. If the Trust believes that a breach of the policy may be a criminal offence the matter will be reported as soon as possible to the appropriate authorities.

1.6. Where the Trust uses the services of a data processor it will ensure that the contract with the processor requires compliance with all the appropriate provisions of the GDPR and the DPA.

1.7. Where the Trust shares data with a third party it shall ensure that there is a lawful basis for any such sharing, that the data subjects are informed of that sharing and that the process is governed by a data sharing agreement that sets out the purposes of sharing and the steps the third party is taking to ensure that the data is processed in accordance with the GDPR and the DPA.

2. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individuals: ● Name (including initials) ● Identification number ● Location data ● Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Term	Definition
Special categories of personal data	This policy applies to all personal data, regardless of whether it is in paper or electronic format. Personal data which is more sensitive and so needs more protection, including information about an individual's: ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs ● Trade union membership ● Genetics ● Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes ● Health – physical or mental ● Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of the processing of personal data. The trust processes personal data relating to parents and carers, pupils, staff, governors, visitors and others, and therefore is a data controller.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
The Trust	Ebor Academy Trust including any of its Academies.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Recognised Legitimate Interests	specific activities (such as safeguarding children, emergency response, or public security) where the DUAA removes the requirement for a balancing test.
Balancing Test	requires an organisation to weigh its own legitimate interests (or those of a third party) against the fundamental rights, freedoms, and interests of the individuals whose data is being processed.

3. Roles and Responsibilities

3.1. Trust Board is responsible for:

- The Trust Board of Trustees has overall responsibility for ensuring that our organisation complies with all relevant data protection obligations.

3.2. Data Protection Officer (DPO) is responsible for:

- Overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable.

- They will provide an annual report of their activities directly to the trust board and, where relevant, report to the board their advice and recommendations on Trust data protection issues.
- The DPO is also the first point of contact for individuals whose data the Trust processes, and for the Information Commission.

Our DPO is the Head of Governance and Compliance and is contactable at dpo@ebor.academy

3.3. Other staff

The Chief Executive and Headteachers act as the representative of the data controller on a day-to-day basis.

All Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Trust of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals in order to complete a Data Protection Impact Assessment

4. The Principles of Data Protection

4.1. This policy sets out the basis upon which the Trust processes personal data in order to be compliant with the UK GDPR and the DPA. Article 5 of the UK GDPR sets out the principles that any processing of personal data must abide by. The principles are that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Trust aims to comply with these principles.

5. Lawful, Fair, and Transparent Data Processing

We will always consider the fairness of our data processing. We will ensure we do not

handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them. Whenever we first collect personal data directly from individuals, we will:-

- provide them with the relevant information required by data protection law via a Privacy Notice
- only collect personal data for specified, explicit and legitimate reasons.
- If we want to use personal data for reasons other than those given when we first obtained the data, we will inform the individuals concerned before we do so and seek consent where necessary.
- If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as the sole basis for processing, we will obtain parental consent (except for online counselling and preventive services).

5.1. The Trust will only process general category personal data where we have one or more 'lawful bases' (legal reasons) under data protection law:

- The data needs to be processed so that the Trust can fulfil **a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract.
- The data needs to be processed so that the Trust can comply with a **legal obligation.**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life.
- The data needs to be processed so that the school, as a public authority, can perform a task in the **public interest** or exercise its official authority.
- The data needs to be processed for the **legitimate interests** of the school or trust (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden. Direct marketing and significant automated decisions are a legitimate interest.
  Processing pupil data to protect welfare or prevent harm is a "Recognised Legitimate Interest" and as such, does not require a balancing test between the trust's aims and the individual's privacy risks.
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent.**

5.2. For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018:-

- The individual (or their parent/carer where appropriate in the case of a pupil) has given their explicit consent
- The data has been "manifestly made public by the Data Subject". For example, by posting it on Twitter
- To carry out rights and obligations under employment law, social security or social protection law
  For example, processing to ensure the health and safety of stakeholders, TUPE, etc.
- To establish, exercise or defend legal claims
- To protect the vital interests of a staff member or other person, where they are legally or physically incapable of giving consent for the assessment of a person's working capacity either on the basis of UK law or under contract with a health professional, such as an external occupational health provider
- The data needs to be processed for reasons of substantial public interest as

defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

6. Data Relating to Criminal Proceedings/Convictions or Child Protection/Safeguarding Issues.

6.1. We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where processing is necessary to carry out our obligations and provided we do so in line with data protection legislation.

6.2. This information is not routinely collected and is only likely to be processed by the Trust in specific circumstances. For example, as a result of an appointment and Disclosure and Barring Service checks, or if information about criminal convictions comes to light during the period of employment of service with the Trust; if a child protection issue arises; or if a parent/carer is involved in a criminal matter.

6.3. Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and/or the Police.

6.4. Such information will only be processed to the extent that it is lawful to do so, and appropriate measures will be taken to keep the data secure.

7. Specified, Explicit, and Legitimate Purposes

7.1. The Trust collects and processes the personal data including:
- Personal data collected directly from data subjects; and
- Personal data obtained from third parties.

7.2. The Trust only collects, processes, and holds personal data for the specific and legitimate purposes (or for other purposes expressly permitted by the UK GDPR).

7.3. Data subjects are kept informed at all times of the purpose or purposes for which the Trust uses their personal data.

8. Adequate, Relevant, and Limited Data Processing

The Trust and its Academies will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

9. Accuracy of Data and Keeping Data Updated

9.1. The Trust shall ensure that all personal data collected, processed, and held by it is kept accurate and up to date. This includes, but is not limited to, the rectification of personal data at the request of a data subject.

9.2. The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

10. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

11. Data Retention

11.1. The Trust and its Academies shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

11.2. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

11.3. For full details of the Trust's approach to data retention, including retention periods for specific personal data types held by the Trust and its Academies, please refer to our Data Retention Policy 19b, which is available on request.

12. Security of Data

The Trust shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

13. Record Keeping

13.1. The Trust and its Academies shall keep written internal records of all personal data collected, held and processing, which shall incorporate the following information:

- Details of the categories of data subject to which that personal data relates;
- Details of how long personal data will be retained by the Trust or Academy (please refer to the Trust's Data Retention Policy); and
- Detailed descriptions of all technical and organisational measures taken by the Trust or Academy to ensure the security of personal data.
- The purposes for which the Trust or Academy collects, holds, and processes the personal data;
- Details of the categories of data subject to which that personal data relates;
- Details of how long personal data will be retained by the Trust or Academy (please refer to the Trust's Data Retention Policy); and
- Detailed descriptions of all technical and organisational measures taken by the Trust or Academy to ensure the security of personal data.

13.2. The Trust, as the overall data controller, is required to be able to demonstrate compliance with the Data Protection Act including the elements of the GDPR contained in the Act. The Trust will demonstrate this compliance through the following documentation:

- The Record of Processing Activities for each Academy and the Trust
- The register of data processors
- A register of any data processed on behalf of other data controllers
- A register of data sharing agreements covering disclosure to other controllers
- A register of data breach incidents including their investigation, mitigation, communications including reporting to the regulator.
- Data Protection Impact Assessments for all initiatives that meet the criteria
- A register of audit activities, including non-compliances and actions taken to mitigate that non-compliance
- A record of the training provided to staff.

14. Data Protection Impact Assessments

14.1. The Trust, as the overall data controller, shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

14.2. Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

- The type(s) of personal data that will be collected, held, and processed;
- The purpose(s) for which personal data is to be used;
- The Trust's or Academy's objectives in bringing forward the initiative;
- How personal data is to be used within the proposed initiative;
- The parties (internal and/or external) who are to be consulted;
- The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- Risks posed to data subjects;
- Risks posed both within and to the Trust or Academy; and
- Proposed measures to minimise and handle identified risks.

14.3. The Trust shall have the power to delegate the compilation of a Data Protection Impact Assessment to an Academy.

15. Keeping Data Subjects Informed

15.1. The Trust shall provide a privacy notice advising how data will be used.

15.2. The following information shall be provided:

- Details of the Trust including, but not limited to, the identity of its Data Protection Officer;
- The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- Where the personal data is to be transferred to one or more third parties, overview of those parties;
- Where the personal data is to be transferred to a third party that is not located in the UK standards are "not materially lower" than UK standards;
- Details of the data subject's rights under the GDPR and DPA;
- Details of the data subject's right to withdraw their consent to the Trust's processing of their personal data at any time to the extent that any such consent applies;
- Details of the data subject's right to complain to the Information Commission (the "supervisory authority" under the GDPR);
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
- Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

16. Data Subject Access Requests

Individuals have a right to make a Subject Access Request (SAR) to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:
- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

- If staff receive a subject access request in any form they must immediately forward it to the DPO.

Children and subject access requests

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

Responding to subject access requests

When responding to requests, the trust is only required to conduct "reasonable and proportionate searches". The Trust may be justified in narrowing or refusing a request if the information is stored in inaccessible archives or retrieval would require disproportionate effort.

We:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or on receipt of the additional information needed to confirm identity, consent where relevant)
- May ask for the request to be targeted or reduced to aid completion within timescales.
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts
- If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.
- When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

17. Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the DPO. Please see the Data Protection Complaint Form (Appendix A)
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)
- Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

18. Parental requests to see the educational record

- In academies, there is no automatic parental right of access to the educational record, but we may choose to provide this. Parents/carers should ask the school if they would like to see their child's educational record.

19. CCTV

Some Ebor schools have CCTV installed. Please refer to school's individual CCTV policy for details of how it is managed. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the School Business Manager.

20. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

21. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. Ebor Academy Trust recognises that AI has many uses to help pupils learn, but also poses risks

to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

Staff and students will be provided with appropriate training surrounding the ethical and responsible use of approved AI tools. This may include training on what data is appropriate to share (e.g. non confidential, non copyrighted material) and on risk minimisation and anonymisation where appropriate.

As generative AI develops, it is recognised that other useful AI tools may appear and staff may want to use these for legitimate purposes. Further AI tools will be assessed on an individual basis by relevant stakeholders, the DPO and IT lead using relevant processes such as a Data Protection Impact Assessment (section 14). Additionally, DPIAs for AI tools will consider the additional AI specific criteria of algorithmic bias, lack of transparency, the use of copyrighted material and data retention within the AI model itself.

There will be meaningful human involvement for any significant decision made by AI, such as grading or flagging at-risk pupils.

All AI tools will also need to be signed off for use by the IT lead as stated in section 33 of the policy. Furthermore, wherever reasonably possible, data inserted into AI tools will be anonymised and always restricted to what is necessary for the tool's specific function. Personal data may only be uploaded to tools which have been approved for this purpose.

22. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies such as AI tools (the DPO will advise on this process). For any online service used by children (e.g., educational apps), the Trust must explicitly account for children's needs and vulnerabilities
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Considering where applicable, if internal and external tools have design that responds to the maturity of the user, promoting privacy by default, data minimisation and restrict sharing (for child users).the Trust will ensure EdTech vendors provide age-appropriate experiences and recognise that children have a lesser understanding of data risks

Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our school and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

23. Rectification of Personal Data

- Data subjects may have the right to require the Trust to rectify any of their personal data that is inaccurate or incomplete.
- Where such rectification is possible, the Trust shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Trust of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
- In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

24. Erasure of Personal Data

24.1. Data subjects have the right to request that the Trust erases the personal data it holds about them in the following circumstances:
- It is no longer necessary for the Trust to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
- The data subject wishes to withdraw their consent to the Trust holding and processing their personal data;
- The data subject objects to the Trust holding and processing their personal data (and there is no overriding legitimate interest to allow the Trust to continue doing so) (see Part 18 of this Policy for further details concerning the right to object);
- The personal data has been processed unlawfully;
- The personal data needs to be erased in order for the Trust to comply with a particular legal obligation; or
- The personal data is being held and processed for the purpose of providing information society services to a child.

24.2. Unless the Trust has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

24.3. In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

25. Restriction of Personal Data Processing

- Data subjects may request that the Trust restricts processing the personal data it holds about them. If a data subject makes such a request, the Trust shall in so far as is possible ensure that the personal data is only stored and not processed in any other fashion.
- If the Trust is required to process the data for statutory purposes (as defined by purposes of processing based on the performance of a public task or substantial public interest) or for reasons of legal compliance, then the Trust shall inform the Data Subject that this processing is expected to take place. If possible, this notice will be provided prior to processing.

- In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

26. Data Portability

- The Trust processes some personal data using automated means. Such processing is carried out by, amongst other things, our management information system(s), our human resources system and our catering management system(s).
- Where data subjects have given their consent to the Trust to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Trust and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data, in a machine readable format, and to use it for other purposes (including transmitting it to other data controllers).
- Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.
- All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.
- Where direct transfer to another data controller is not possible the personal data will be provided in a commonly used form such as comma separated values (.csv)
- The data that can be transferred is restricted to that which has been provided by the data subject.

27. Objections to Personal Data Processing

- A data subject has the right to object, on grounds relating to his or her particular situation, to processing of personal data which is processed based on the performance of a public task or the Legitimate Interests of the Trust.
- The Trust shall no longer process the personal data unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
- Where personal data is processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
- Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
- If the Trust engages in scientific or historical research, the DUAA allows for "broad consent". Where a data subject objects to the Trust processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". The Trust is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest. Personal information can be re-used for research without a new privacy notice if providing one would involve "disproportionate effort

28. Profiling

- The Trust uses personal data for profiling purposes. These purposes relate to helping pupils maximise achievement and attendance.
- When personal data is used for profiling purposes, the following shall apply:
- Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;
- The Trust will use appropriate mathematical or statistical procedures

- The Trust will implement technical and organisational measures to minimise the risk of errors.
- All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling.

29. Personal Data Collected, Held, and Processed

The Trust uses a wide range of personal data across many processes. More detail can be found in our privacy notices. If you wish to view the complete lists of categories of personal data we process please contact our Data Protection Officer.

30. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept secure when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, or on staffroom tables, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must take care of the data with appropriate security measures.
- Passwords that are at least 8 characters long containing upper and lowercase letters and a number or symbol are used to access school computers, laptops and other electronic devices. Staff are reminded that they should not reuse passwords from other sites and passwords used in the previous 10 occasions cannot be used again.

  There is an enforced minimum password age:

  - users can't change password for the first day after a password change,
  - users will be forced to change their password on a PC after 90 days

When accessing the system remotely, multiple factor authentication is enforced.

Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.

Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

31. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

32. Data Security - Use of Personal Data

- No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Trust requires access to any personal data that they do not already have access to, such access should be formally requested from the data processor.
- No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Trust or not, without the initial authorisation of the data processor and Trust Data Protection officer.
- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time.
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it
- Where personal data held by the Trust is used for marketing purposes, it shall be the responsibility of the trust member of staff processing the data for marketing purposes to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

33. Data Security - IT Security

- The Trust requires that any passwords used to access personal data shall have a minimum of [12] characters, composed of a mixture of upper and lower case characters, numbers and symbols. Passwords are not expected to be changed upon a regular basis but users will be expected to change their password if instructed by the Trust;
- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Trust, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Trust's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and
- No software may be installed on any Company-owned computer or device without the prior approval of Ebor's IT Lead.
- Where members of staff or other users use online applications that require the use of personal data, the use of that application must be signed off by Ebor's IT Lead.

34. Organisational Measures

- All employees, agents, contractors, or other parties working on behalf of the Trust shall be made fully aware of both their individual responsibilities and the Trust's responsibilities under the GDPR and under this Policy, and shall have free access to a copy of this Policy.
- Only employees, agents, sub-contractors, or other parties working on behalf of the Trust that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Trust.
- All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be appropriately trained to do so.
- All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be appropriately supervised.
- All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in

the workplace or otherwise.

- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.
- All personal data held by the Trust shall be reviewed periodically, as set out in the Trust's Data Retention Policy.
- The performance of those employees, agents, contractors, or other parties working on behalf of the Trust handling personal data shall be regularly evaluated and reviewed.
- The contravention of these rules may be treated as a disciplinary matter.
- All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract.
- All agents, contractors, or other parties working on behalf of the Trust handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Trust arising out of this Policy and the GDPR
- Where any agent, contractor or other party working on behalf of the Trust handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Trust against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

35. Transferring Personal Data to a Country Outside the UK

35.1. The Trust may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the UK.

35.2. The transfer of personal data to a country outside of the UK shall take place only if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that ensures an adequate level of protection for personal data;
- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies;
- The transfer is made with the informed consent of the relevant data subject(s);
- The transfer is necessary for the performance of a contract between the data subject and the Trust (or for pre-contractual steps taken at the request of the data subject);
- The transfer is necessary for important public interest reasons;
- The transfer is necessary for the conduct of legal claims;
- The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
- The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

36. Data Breach Notification Add timelines

36.1. All personal data breaches must be reported immediately to the Trust's Data Protection Officer and managed in compliance with the Data Breach Management Policy 19a.

36.2. If a personal data breach occurs and that breach is likely to result in a risk to the

rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commission is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

36.3. In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

37. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

38. Complaints

The **Data (Use and Access) Act 2025 (DUAA)** introduced a statutory requirement for a formal internal data protection complaints mechanism.

Please complete the form at Appendix A if you would like to complain about GDPR procedures. The trust. The Data Protection Officer will acknowledge the complaint within 30 days, take appropriate steps to investigate the complaint, inform the data subject of the outcome *without undue delay* and ensure a clear audit trail for the process.

39. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Privacy notices
- CCTV
- Data Breach Policy

40. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR
- The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)
- Data (Use and Access) Act 2025 (DUAA)
- The statutory Age Appropriate Design Code (ICO)
- Keeping Children Safe in Education

It is based on guidance published by the Information Commission on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

Appendix A

Formal Data Protection Complaint Form

Under the UK GDPR and the Data (Use and Access) Act 2025 (DUAA)

This form is for you to raise concerns about how **[Your Organisation Name]** has handled your personal data or your data protection rights. We will acknowledge receipt of your complaint within 30 days and provide a full response without undue delay.

Please complete all sections clearly to help us investigate and resolve your concerns promptly.

Section 1: Your Details (The Complainant)

Field	Required Information
Title (Mr/Mrs/Ms/Other)	
First Name(s)	
Last Name(s)	
Address	
Postcode	
Primary Contact Number	
Email Address	
Are you complaining on behalf of someone else e.g. your child?	**Yes -** please complete Section 2 and provide written authority.) **No**

Section 2: Details of the Data Subject (If different from Complainant)

If you are complaining on behalf of a third party, you must provide a signed Letter of Authority or other proof of legal representation. If you are the data subject, please skip to Section 3.

Field	Required Information
Full Name of Data Subject	
Relationship to Data Subject	
Confirmation of Authority	**I confirm that a Letter of Authority/Proof of Representation is attached. Yes or I confirm the data subject is under 12**

Section 3: Details of Your Complaint

A. Nature of the Complaint

Please select the category that best describes your complaint. You can select more than one.

Category	Select
Access/Subject Access Request (SAR)	Not received a response, or the response was late/incomplete.
Erasure/Deletion (Right to be Forgotten)	Refusal to delete my data, or data remains after a request for deletion.

Rectification	Personal data held about me is inaccurate or incomplete, and a request to correct it has been ignored or refused.
Unlawful Processing	My data has been processed (collected, stored, used) without a valid legal basis or consent.
Security/Data Breach	My personal data has been lost, stolen, or improperly disclosed.
Transparency/Privacy Information	The privacy notice/information provided was unclear, incomplete, or misleading.
Automated Decision-Making	Objecting to a decision made solely by automated means without human involvement (DUAA).
Other Data Protection Right	Specify:

B. Description of the Complaint

Please clearly and simply explain what happened, when it happened, and how you believe Ebor Academy Trust has failed to comply with data protection law. Please use additional sheets if necessary.

(Date(s) the incident occurred or when you first became aware):

(Full Description of Complaint - include specific data, names, and departments if known):

C. Desired Outcome

*What would you like **[Your Organisation Name]** to do to resolve your complaint?*

Desired Action	Select
Correct or update my personal data.	
Delete my personal data.	
Provide me with my personal data.	
Stop processing my personal data in a specific way.	
Provide a full explanation and apology.	
Other (Please specify below):	

Section 4: Supporting Documentation

Document Type	Provided (Yes/No)
Proof of Identity (if requested by the DPO)	Yes / No
Letter of Authority (if applicable)	Yes / No
Other evidence (e.g., screenshots, email trails)	Yes / No

Total number of documents/pages attached:

Section 5: Declaration and Consent

By signing and submitting this form, I confirm that:

1. The information provided in this complaint form is accurate and complete to the best of my knowledge.
2. I understand that Ebor Academy Trust will process the personal data contained in this form only for the purposes of investigating and responding to my complaint, in accordance with our Data Protection Policy.

Signature of Complainant	
Date	

Submitting Your Complaint

Please send the completed form and any supporting documents to the Data Protection Officer (DPO) at **Ebor Academy Trust** via:

Method	Contact
Email	dpo@ebor.academy
Post	Wendy Harrington, Ebor Academy Trust, The Leyes, Osbaldwick Yo10 3PR

Our Commitment to You:

- Acknowledgement: We will acknowledge receipt of your complaint within 30 days.
- Response: We will conduct an appropriate investigation and provide you with an outcome without undue delay.

If you are dissatisfied with our response, you have the right to refer your complaint to the Information Commission.