EBOR ACADEMY TRUST

**Policy Number**

19

# Data Protection Policy

| | |
|---|---|
| **Approved By:** | Ebor Academy Trust Board of Trustees |
| **Approval Date:** | November 2022 |
| **Review Period:** | Every 2 years (subject to legislative/regulatory changes) |
| **Review Date:** | November 2023 |

| | |
|---|---|
| ***Author:*** | Wendy Harringotn Head of Governance & Compliance |
| ***Date Created/updated:*** | *November 2022* |
| ***Version Number:*** | *3* |

**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) 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 Academies 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 Academies 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.<br><br>This may include the individuals:<br>● Name (including initials)<br>● Identification number<br>● Location data<br>● Online identifier, such as a username<br><br>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. |

| | |
|---|---|
| **Special categories of personal data** | Personal data which is more sensitive and so needs more protection, including information about an individual's:<br>● Racial or ethnic origin<br>● Political opinions<br>● Religious or philosophical beliefs<br>● Trade union membership<br>● Genetics<br>● Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>● Health – physical or mental<br>● 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.<br>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. |
| **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. |

## 3. Roles and Responsibilities

3.1. Trust Board is responsible for:

- The Trust Board of Trustees (through its Local Governing Committees) 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 our 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 governing 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 ICO. Full details of the DPO's responsibilities are set out in their job description.

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

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

3.4. 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 If they need help with any contracts or sharing personal data with third parties

## 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 DPA. Article 5 of the UK GDPR sets out the principles that any processing of personal data must abide by. The principles say 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.

4.2. This policy sets out, in Sections 4- 13, how the Trust complies with the principles of data protection and the requirement for data protection by default and design. Sections 14-23 describe how the Trust supports the rights of data subjects. Finally, Sections 24 – 31 describe how the Trust ensures the security of personal data being processed and how it deals with any failures that result in a data breach

## 5. Lawful, Fair, and Transparent Data Processing

5.1. The Trust will only process general category personal data where we have one or more 'lawful bases' (legal reasons) to do so 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 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. 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
- Certain special category data may only be processed if the data controller has a lawful basis under both Article 6 and Article 9 of the UK GDPR, and one associated Data Protection Act (2018) Schedule 1 condition.

## 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.

6.5. 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 in all instances (except for online counselling and preventive services).

## 7. Specified, Explicit, and Legitimate Purposes

7.1. The Trust collects and processes the personal data set out in Part 23 of this Policy. This includes:

- 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 purposes set out in Part 23 of this Policy (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. Please refer to Part 14 for more information on keeping data subjects informed.

## 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) as under Part 5, above, and as set out in Part 23, below.

## 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, as set out in Part 16, below.

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. Data Retention

10.1. 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.

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

10.3. 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.

## 11. 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. Further details of the technical and organisational measures which shall be taken are provided in Parts 22 to 27 of this Policy.

## 12. Record Keeping

12.1. The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Trust's other data protection-related policies, and with the GDPR and other applicable data protection legislation. It shall be for the Trust and its Academies to provide suitable records to enable this monitoring to take place.

12.2. The Trust and its Academies shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- The name and details of the Trust or Academy, its Data Protection Officer, and any applicable third-party data processors;
- The purposes for which the Trust or Academy collects, holds, and processes personal data;
- Details of the categories of personal data collected, held, and processed by the Trust or Academy, and the categories of data subject to which that personal data relates;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- 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.

12.3. 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 and associated contracts
- 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 record of completion of compliance activities based on best practice published by the Regulator
- A register of audit activities, including non-compliances and actions take to mitigate that non-compliance
- A record of the training provided to all staff.

## 13. Data Protection Impact Assessments

13.1. 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.

13.2. 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.

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

## 14. Keeping Data Subjects Informed

14.1. The Trust shall provide the information set out in Part 12.2 to every data subject:

- Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
- Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
    - if the personal data is used to communicate with the data subject, when the first communication is made; or
    - if the personal data is to be transferred to another party, before that transfer is made; or
    - as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

14.2. 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 (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;
- Where applicable, the legitimate interests upon which the Trust is justifying its collection and processing of the personal data;
- 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, details of those parties;
- Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details);
- Details of data retention;
- 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 Commissioner's Office (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.

## 15. Data Subject Access Requests

15.1. Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Trust holds about them, what it is doing with that personal data, and why.

15.2. Employees wishing to make a SAR should contact the trust Data Protection officer (dpo@ebor.academy)

15.3. Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

15.4. Responses to SARs shall be dependent upon the terms of the GDPR, the Data Protection Act (2018) and associated ICO guidance.

15.5. The Trust does not charge a fee for the handling of normal SARs. The Trust reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

## 16. Rectification of Personal Data

16.1. Data subjects may have the right to require the Trust to rectify any of their personal data that is inaccurate or incomplete.

16.2. 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.

16.3. 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.

## 17. Erasure of Personal Data

17.1. 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.

17.2. 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.

17.3. 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).

## 18. Restriction of Personal Data Processing

18.1. 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.

18.2. 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.

18.3. 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).

## 19. Data Portability

19.1. 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).

19.2. 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).

19.3. Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

19.4. 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.

19.5. 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)

19.6. The data that can be transferred is restricted to that which has been provided by the data subject.

## 20. Objections to Personal Data Processing

20.1. 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.

20.2. 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.

20.3. 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.

20.4. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

20.5. 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.

## 21. Automated Decision-Making

21.1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

21.2. The Trust may make decisions based on automated processing if that processing:

- is necessary for entering into, or performance of, a contract between the data subject and the Trust;
- is authorised by Union or Member State law to which the Trust is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- is based on the data subject's explicit consent.

21.3. Where a data subject is unhappy with the outcome of a decision based on automated processing, the Trust will provide the opportunity for the decision to be reviewed by a person with appropriate authority to reflect the circumstances of the data subject. The Trust's decision will be final.

21.4. The Trust will not use special category personal data to make decisions based on automated processing unless the data subject has given explicit consent or for reasons of substantial public interest. The Trust will ensure that the rights and freedoms of data subjects are safeguarded if such processing takes place.

## 22. Profiling

22.1. The Trust uses personal data for profiling purposes. These purposes relate to helping pupils maximise achievement and attendance.

22.2. 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.

22.3. All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 to 26 of this Policy for more details on data security).

## 23. 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.

## 24. Data Security - Transferring Personal Data and Communications

24.1. Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

24.2. The Trust will ensure that where special category personal data or other sensitive information is sent in the post that it shall be possible to demonstrate that it was delivered.

24.3. Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

24.4. Where special category personal data or other sensitive information is to be sent by e-mail the email will either be sent using a suitable encryption method or the data will be sent in an attached, encrypted document and not in the body of the e-mail.

24.5. Where personal data is to be transferred in removable storage devices, these devices shall be encrypted. The use of unencrypted removable storage devices is prohibited by the Trust

24.6. Where personal data is being sent by email outside of the Trust is must be secured at minimum by password protection or by the use of an appropriate encryption system.

25. **Data Security - Storage**

25.1. All electronic copies of personal data should be stored securely using passwords, user access rights and where appropriate data encryption;

25.2. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

25.3. All personal data relating to the operations of the Trust, stored electronically, should be backed up on a regular basis

25.4. Where any member of staff stores personal data on a mobile device (whether that be computer, tablet, phone or any other device) then that member of staff must abide by the Acceptable Use policy of the Trust. The member of staff shall also ensure that they can provide a secure environment for that device to be used to minimise any risk to the confidentiality or integrity of the information.

## 26. Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Trust's Data Retention Policy.

## 27. Data Security - Use of Personal Data

27.1. 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.

27.2. 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.

27.3. 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.

27.4. 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

27.5. 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.

## 28. Data Security - IT Security

28.1. 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;

28.2. 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;

28.3. 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

28.4. No software may be installed on any Company-owned computer or device without the prior approval of Ebor's IT Lead.

28.5. Where members of staff or other user use online applications that require the use of personal data, the use of that application must be signed off by Ebor's IT Lead.

## 29. **Organisational Measures**

29.1. 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.

29.2. 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.

29.3. All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be appropriately trained to do so.

29.4. All employees, agents, contractors, or other parties working on behalf of the Trust handling personal data will be appropriately supervised.

29.5. 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.

29.6. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.

29.7. All personal data held by the Trust shall be reviewed periodically, as set out in the Trust's Data Retention Policy.

29.8. 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.

29.9. The contravention of these rules may be treated as a disciplinary matter.

29.10. 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.

29.11. 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

29.12. 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.

## 30. Transferring Personal Data to a Country Outside the UK

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

30.2. The transfer of personal data to a country outside of the EEA 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 the European Commission has determined 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; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
- 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.

## 31. Data Breach Notification Add timelines

31.1. 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.

31.2. 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 Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

31.3. 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.

31.4. Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of the Trust's data protection officer (or other contact point where more information can be obtained).
- The likely consequences of the breach.
- Details of the measures taken, or proposed to be taken, by the Trust to address the breach including, where appropriate, measures to mitigate its possible adverse effects