Data Protection Policy

Embrace Multi Academy Trust strives to maintain and improve good provision and outcomes at each of its member schools. Based upon our shared ethos and our values of wisdom, collaboration, respect, integrity, inclusivity and compassion, we aim to support the learning and development of every person within the trust, and our policies are written from this perspective.

Version	Approval Level	Document History	Date	Review Period
V1	Trust Leader	Approved	01/09/2023	Annual
V2	Trust Leader	Approved	01/10/2024	Annual
V3	Trust Leader	Approved	01/08/2025	Annual

1. Introduction

1.1. Embrace Multi Academy Trust and its schools are committed to working effectively to provide a secure environment to protect the data that we hold and store. Whilst there is a statutory duty that is important, the fact that we store data about individuals means that we are responsible for your data, and we take that very seriously. This policy and the privacy notices set out how we look after and use data.

1.2. Each school is responsible for the day-to-day management of data that is held about pupils, staff, parents, carers, and other individuals in connection with that school.

1.3. The trust central team is responsible for data held centrally about individuals.

1.4. Where we use the phrase 'we', that refers to the trust and the individual schools.

2. What Is The General Data Protection Regulation (UK GDPR)?

2.1. This is a European directive that was brought into UK law with an updated Data Protection Act 2018 (DPA) in May 2018. It was brought into line with changes to the UK leaving the EU on 31 December 2020.

2.2. The UK GDPR and DPA 2018 exist to look after individuals' data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure.

2.3. The UK GDPR exists to protect individual rights in an increasingly digital world.

3. Who Does UK GDPR Apply To?

3.1. Everyone, including schools. As 'public bodies' schools and trusts have more obligations than some small businesses. It is mandatory to comply with the UK GDPR and provisions in the Data Protection Act 2018.

3.2. We want to make sure information about pupils, parents, staff and volunteers is kept secure and within the law.

4. What Is Data?

4.1. Any information that relates to a living person that identifies them. This can be by name, address or telephone number for example. It also relates to details about that person, which can include opinions.

4.2. Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

4.3. Schools often collect sensitive data for Department for Education (DfE) and local authority (LA) requirements and, of course, pupil data may contain information about safeguarding, SEND or health needs. Information about other family members may also be on the school file.

4.4. Privacy notices that explain how data about specific groups or activities is used

and stored are also available. These can be obtained from each school and links on the school website to UK GDPR compliance.

5. What Are The Key Principles Of The UK GDPR?

5.1. Lawfulness, transparency and fairness

Schools must have a legitimate reason to hold the data, and we explain this in the data privacy notices. We often ask for consent to use data about a pupil for a particular purpose. If you wish to withdraw consent, we have a form to complete to allow us to process your request. There are some times when you cannot withdraw consent, as explained in the section on 'Data Subjects' Rights'.

5.2. Collect data for a specific purpose and use it for that purpose

Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

5.3. Limited collection

Data controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack, only limited information can then be lost.

5.4. Accuracy

Data collected should be accurate, and steps should be taken to check and confirm accuracy. This is done when pupils join the school and is reviewed on an annual basis.

If a data subject feels that the information held is inaccurate, or should no longer be held by the controller, or should not be held by the controller in any event, an approach should be made directly to the individual school. A dispute resolution process and complaint process can be accessed, using the relevant forms.

5.5. Retention

A records management retention policy is in place that governs how long records are held for.

5.6. Security

Processes are in place to keep data safe, which might be paper files, electronic records or other information. Please see the trust Information Security Policy for more information.

6. Who Is A 'Data Subject'?

6.1. Any individual whose details we keep on file. Some details are more sensitive than others. The UK GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.

7. Data Subjects' Rights

7.1. Individuals have a right:

- to be informed
- of access to data stored about them or their children
- to rectification, if there is an error on the data stored

- to erasure, if there is no longer a need for school to keep the data
- to restrict processing, ie to limit what is done with their data
- to object to data being shared or collected.

7.2. There are other rights that relate to automated decision making and data portability that are not directly relevant in schools.

7.3. Data subjects' rights are also subject to child protection and safeguarding concerns and sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the DfE, Social Care, the LA and HMRC amongst others. In some cases, these obligations override individual rights.

7.4. These data subjects' rights are set out in more detail in the GOV.UK document 'My Rights – A Guide for Data Subjects'.

8. Subject Access Requests

8.1. You can ask for copies of information that we hold about you or a pupil (who you have parental responsibility for). A Subject Access Request form can be found on the trust website here. This needs to be completed and returned to the relevant school's named individual responsible for UK GDPR (details via the previous link). You may need to provide identification evidence for us to process the request.

8.2. We have to provide the information within a month, but this can be extended if the request is complicated, or the data cannot be accessed. It may be necessary for us to extend the response period when requests are submitted over the summer holidays. This is in accordance with article 12(3) of the UK GDPR and will be the case where the request is complex, for example, where we need multiple staff to collect the data.

8.3. When we receive a request, we may ask you to be more specific about the information that you require. This is to refine any queries to make sure you access what you need, rather than getting a lot of information that may not be relevant to your query.

8.4. In some cases, we cannot share all information we hold on file, for example if there are contractual, legal or regulatory reasons.

8.5. We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, eg school nurses who are employed by the NHS.

8.6. We will supply the information by paper or electronic form.

8.7. If you wish to complain about the process, please see our Complaints Policy and later information in this policy.

9. Who Is A 'Data Controller'?

9.1. Embrace Multi Academy Trust is the data controller and has ultimate responsibility for how the schools and trust central team manage data. It delegates this processing to individuals to act on their behalf, ie the trust central team and the relevant school staff in each setting.

9.2. The data controller can also have contracts and agreements in place with outside

agencies who are data processors.

10. Who Is A 'Data Processor'?

10.1. This is a person or organisation that uses, collects, accesses, or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a third-party company, possibly a governor, a contractor or temporary employee. It can also be another organisation, such as the police or the LA.

10.2. Data controllers must make sure that data processors are as careful about the data as the controller themselves. The UK GDPR places additional obligations on organisations to make sure that data controllers require contractual agreements to ensure that this is the case.

11. Processing Data

11.1. Embrace and its schools must have a reason to process the data about an individual. Our privacy notices set out how we use data. The UK GDPR has six conditions for lawful processing and any time we process data relating to an individual, it is within one of those conditions.

11.2. If there is a data breach, we have a separate Breach and Non-Compliance Procedure to follow to take immediate action to remedy the situation as quickly as possible.

11.3. The legal basis and authority for collecting and processing data in school are:

- consent obtained from the data subject or their parent
- performance of a contract where the data subject is a third party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law.

11.4. In addition, any special categories of personal data are processed on the grounds of:

- explicit consent from the data subject or about their child
- being necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data.

11.5. Processing data is recorded within the school systems.

12. Data Sharing

12.1. Data sharing is done within the limits set by the UK GDPR. Guidance from the DfE, health, police, LA and other specialist organisations may be used to determine whether data is shared.

12.2. The basis for sharing or not sharing data is recorded in school.

13. Breaches and Non-Compliance

13.1. If there is non-compliance with this policy or processes, or if there is a DPA breach as described within the UK GDPR and DPA 2018, then the guidance set out in the Breach and Non Compliance Procedure (Appendix 1) needs to be followed.

13.2. Protecting data and maintaining data subjects' rights is the purpose of this policy and associated procedures.

14. Consent

14.1. As a trust, where required, we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.

14.2. Consent is defined by the UK GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

14.3. We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

14.4. This will largely be managed in individual schools.

14.5. **Consent and Renewal**

On the Embrace website we have 'privacy notices' that explain how data is collected and used. It is important to read those notices as they explain how data is used in detail.

Obtaining clear consent, where required, and ensuring that the consent remains in place is important for schools. We also want to ensure the accuracy of that information.

14.6. **For Pupils and Parents/Carers**

On joining an Embrace school, parents will be asked to complete a form (paper or digital) giving next-of-kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in-school purposes, as set out on the data collection/consent form.

The contact and consent form are reviewed on an annual basis. It is important to inform the school if any details, or your decision about consent, changes via a form available from the school. It is the obligation of each individual to notify the school of changes.

14.7. **Pupil Consent Procedure**

Where processing relates to a child under 13 years of age, the school will obtain consent from a person who has parental responsibility for the child as required.

Pupils may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

14.8. **Withdrawal of Consent**

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent, the school will consider each situation on the merits and within the principles of UK GDPR and also child welfare, protection and safeguarding principles. You must complete the appropriate form.

15. CCTV Policy

15.1. Where CCTV is used, schools will also publish a CCTV policy on their individual websites. We use CCTV and store images for a period of time in line with the policy. CCTV may be used for:

- detection and prevention of crime
- school staff disciplinary procedures
- pupil behaviour and suspension/exclusion management processes
- assisting the school in complying with legal and regulatory obligations.

16. Data Protection Officer

16.1. We have a Data Protection Officer whose role is:

- to inform and advise the data controller or the data processor and the employees who carry out processing of their obligations under the UK GDPR
- to monitor compliance with the UK GDPR and DPA
- to provide advice where requested about the data protection impact assessment and monitor its performance
- to be the point of contact for data subjects if there are concerns about data protection
- to cooperate with the supervisory authority and manage the breach procedure
- to advise about training and CPD for the UK GDPR.

16.2. Our DPO is John Walker, The Brutus Centre, Station Road, Totnes, Devon, TQ9 5RW. Email: Info@phplaw.co.uk, Phone: 03337 729763

17. Physical Security

17.1. As a trust, we are obliged to have appropriate security measures in place.

17.2. In school, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, ie locked offices and cupboards that contain personal data should be secured if the processor is

not present.

17.3. The records are in secured cabinets with only appropriate members of staff having access.

17.4. All staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

17.5. All sites and locations need to have the suitable security and review measures in place.

18. Secure Disposal

18.1. When disposal of items is necessary, a suitable process must be used. This is to secure the data and to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

18.2. These processes, when undertaken by a third party are subject to contractual conditions to ensure UK GDPR and DPA compliance.

19. Complaints & the Information Commissioner's Office (ICO)

19.1. The Embrace Complaints Policy deals with complaints about data protection issues.

19.2. There is a right to complain if you feel that data has been shared without consent or lawful authority.

19.3. You can complain if you have asked to us to erase, rectify, or not process data and we have not agreed to your request.

19.4. We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the form, and we will contact you with more details about the timescale and process.

19.5. In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations (email: casework@ico.org.uk / helpline: 0303 123 1113 / web: www.ico.org.uk)

20. Review

20.1. A review of the effectiveness of UK GDPR compliance and processes will be conducted by the Data Protection Officer every 12/24 months.

Appendix 1: Breach and Non-Compliance Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

1. On finding or causing a breach, or potential breach, the staff member must immediately notify the UK GDPR contact for their school.

2. The UK GDPR contact for the school will then report the breach to the Trust Estates and Compliance Manager.

3. The Trust Estates and Compliance Manager will then liaise with the DPO. The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - lost
    - stolen
    - destroyed
    - altered
    - disclosed or made available to unauthorised people.

4. The DPO will alert the headteacher and the chair of governors of breaches where an individual's rights and freedoms have been or may be affected without undue delay.

5. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary (actions relevant to specific data types are set out at the end of this procedure).

6. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

7. The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (eg, emotional distress), including through:
    - loss of control over their data
    - discrimination
    - identify theft or fraud
    - financial loss
    - unauthorised reversal of pseudonymisation (for example, key-coding)
    - damage to reputation
    - loss of confidentiality
    - any other significant economic or social disadvantage to the individual(s) concerned. If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

8. The DPO will document the decision (either way), in case it is challenged at a later date by the ICO, or an individual affected by the breach. Documented decisions are stored on the headteacher's computer system within the school and the online Go-GDPR portal provided by the DPO service.

9. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned
- the categories and approximate number of personal data records concerned
- the name and contact details of the DPO
- a description of the likely consequences of the personal data breach
- a description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

10. If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

11. The DPO will also assess the risk to individuals, based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - a description, in clear and plain language, of the nature of the personal data breach
    - the name and contact details of the DPO
    - a description of the likely consequences of the personal data breach
    - a description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned. As above, any decision on whether to contact individuals will be documented by the DPO.

12. The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

13. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - facts relating to the breach
    - effects
    - action taken to contain it and to ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
    - records of all breaches which will be stored in a central database by Embrace.

14. The headteacher and UK GDPR contact will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible and will include input from the DPO.

15. **Actions to minimise the impact of data breaches**

    - We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

16. **Sensitive information being disclosed via email (including safeguarding records)**

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the UK GDPR contact in school as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the UK GDPR contact in school will ask the ICT department to recall it.
- In any cases where the recall is unsuccessful, the UK GDPR contact in school will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The UK GDPR contact in school will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The UK GDPR contact in school will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- Advice will be sought from the DPO if any breach is committed and acted upon accordingly.