Data Protection Policy

EBN Academy

Created:		
Reviewed:	**LGB**	**March 22**
Ratified:	**Full Board**	**Signed:**

Data Protection Policy

This policy is drafted in accordance with the requirements of the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 (DPA). It also meets the requirements of the Protection of Freedoms Act 2012. This policy links with our:

- Privacy Notices;
- Retention Schedule;
- ICT acceptable use Policy; and
- CCTV Procedures

Contents

1 Policy statement

1.1 Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as a Trust we will determine how we collect, store and **process personal data** about our pupils, **workforce**, parents and other individuals. This makes us a **data controller** in relation to that **personal data**.

1.2 We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

1.3 All members of our **workforce** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

2 About this policy

2.1 The types of **personal data** that we may be required to handle include information about pupils, parents, our **workforce**, and other individuals that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in the UK General Data Protection Regulation ('**UKGDPR**'), the Data Protection Act 2018, and other regulations (together '**Data Protection Legislation**').

2.2 This policy and any other documents referred to in it set out the basis on which we will **process** any **personal data** we collect from **data subjects**, or that is provided to us by other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out our expected standards for our **workforce** when we process **personal data**.

3 Definition of data protection terms

3.1 All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in the Annex to this policy.

4 Data Protection Officer

As a Trust we are required to appoint a Data Protection Officer ("DPO"). Our DPO is Services4Schools Ltd and they can be contacted at:

EBN Trust
C/O EBN Academy 2
10 High Street
Birmingham
B35 7PR

Or via email: DPO@EBNFS.org

4.1 The DPO is responsible for supporting the Trust with all matters of compliance with the Data Protection Legislation and with this policy. Any questions about

the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

4.2 The DPO is also the central point of contact for all **data subjects** and others in relation to matters of data protection.

5 Data protection principles

5.1 Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:

5.1.1 **Processed** fairly and lawfully and transparently in relation to the **data subject**;

5.1.2 **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes;

5.1.3 Adequate, relevant and not excessive for the purpose;

5.1.4 Accurate and up to date;

5.1.5 Not kept for any longer than is necessary for the purpose; and

5.1.6 **Processed** securely using appropriate technical and organisational measures.

5.2 **Personal Data** must also:

5.2.1 be **processed** in line with **data subjects'** rights;

5.2.2 not be transferred to people or organisations situated in other countries without adequate protection.

5.3 We will comply with these principles in relation to any **processing** of **personal data** by the Trust.

6 Fair and lawful processing

6.1 Data Protection Legislation is not intended to prevent the **processing** of **personal data**, but to ensure that it is done fairly and without adversely affecting the rights of the **data subject**.

6.2 For **personal data** to be **processed** fairly, **data subjects** must be made aware:

6.2.1 that the **personal data** is being **processed**;

6.2.2 why the **personal data** is being **processed**;

6.2.3 what the lawful basis is for that **processing** (see below);

6.2.4 whether the **personal data** will be shared, and if so with whom;

6.2.5 the period for which the **personal data** will be held;

6.2.6 the existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and

6.2.7 the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

6.3 We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any **processing**.

6.4 For **personal data** to be **processed** lawfully, it must be **processed** on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally **process personal data** under the following legal grounds:

6.4.1 where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;

6.4.2 where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g. the Education Act 2011, or statutory guidance like Keeping Children Safe In Education);

6.4.3 where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest, such as the delivery of teaching and learning; and

6.4.4 where none of the above applies then we will seek the consent of the **data subject** to the **processing** of their **personal data.**

6.5 When **special category personal data** is being processed then an additional legal ground must apply to that processing. We will normally only **process special category personal data** under following legal grounds:

6.5.1 where the **processing** is necessary for employment law purposes, for example in relation to sickness absence;

6.5.2 where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;

6.5.3 where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and

6.5.4 where none of the above applies then we will seek the consent of the **data subject** to the **processing** of their **special category personal data**.

6.6 We will inform **data subjects** of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

6.7 If any **data user** is in doubt as to whether they can use any **personal data** for any purpose then they must contact the DPO before doing so.

Vital Interests

6.8 There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** in order to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not in a position to give consent to the **processing**. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

6.9 Where none of the other bases for **processing** set out above apply then the school must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.

6.10 There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

6.11 When pupils and or our **workforce** join the Trust a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

6.12 Whilst we will generally seek consent directly from all pupils due to them being over the age of 12 years old, we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from and individual with parental responsibility.

6.13 If consent is required for any other **processing** of **personal data** of any **data subject** then the form of this consent must:

6.13.1 Inform the **data subject** of exactly what we intend to do with their **personal data**;

6.13.2 Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and

6.13.3 Inform the **data subject** of how they can withdraw their consent.

6.14 Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent.

6.15 The DPO must always be consulted in relation to any consent form before consent is obtained.

6.16 A record must always be kept of any consent, including how it was obtained and when.

7 Processing for limited purposes

7.1 In the course of our activities as a Trust, we may collect and **process** the **personal data** set out in our Information Asset Register, which serves as a schedule of processing activities. This may include **personal data** we receive

directly from a **data subject** (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and **personal data** we receive from other sources (including, for example, local authorities, other schools, parents, other pupils or members of our **workforce**).

7.2 We will only **process personal data** for the specific purposes set out in our Schedule of Processing Activities (an Information Asset Register) or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

8 Notifying data subjects

8.1 If we collect **personal data** directly from **data subjects**, we will inform them about:

8.1.1 our identity and contact details as **Data Controller** and those of the DPO;

8.1.2 the purpose or purposes and legal basis for which we intend to **process** that **personal data**;

8.1.3 the types of third parties, if any, with which we will share or to which we will disclose that **personal data**;

8.1.4 whether the **personal data** will be transferred outside the UK and if so the safeguards in place;

8.1.5 the period for which their **personal data** will be stored, by reference to our Records Management and Retention Policy;

8.1.6 the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making; and

8.1.7 the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

8.2 Unless we have already informed **data subjects** that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive **personal data** about a **data subject** from other sources, we will provide the **data subject** with the above information as soon as possible thereafter, informing them of where the **personal data** was obtained from.

8.3 The Trust will be provided with information relating to third parties in the form of emergency contact details. These individuals must be provided with the information above. Parents are required to obtain the consent of any third party whose details they provide to the Trust for these purposes.

9 Adequate, relevant and non-excessive processing

9.1 We will only collect **personal data** to the extent that it is required for the specific purpose notified to the **data subject**, unless otherwise permitted by Data Protection Legislation.

10 **Accurate data**

10.1 We will ensure that the Trust takes every measure to ensure the **personal data** we hold is accurate and kept up to date.

10.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

10.3 **Data subjects** have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

11 **Timely processing**

11.1 We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all **personal data** which is no longer required.

12 **Processing in line with data subject's rights**

12.1 We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:

12.1.1 request access to **personal data** we hold about them;

12.1.2 object to the **processing** of their **personal data**, including the right to object to direct marketing;

12.1.3 have inaccurate or incomplete **personal data** about them rectified;

12.1.4 temporarily restrict **processing** of their **personal data**;

12.1.5 where possible, to have **personal data** we hold about them erased

12.1.6 have their **personal data** transferred where it is held in a portable form; and

12.1.7 object to the making of decisions about them by automated means.

13 **The Right of Access to Personal Data**

13.1 **Data subjects** may request access to **personal data** we hold about them. Such requests will be considered in line with the Trust's Subject Access Request Procedure.

14 **The Right to Object**

14.1 In certain circumstances **data subjects** may object to us **processing** their **personal data**. This right may be exercised in relation to **processing** that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

14.2 An objection to **processing** does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the **data subject**.

14.3 Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

14.4 In respect of direct marketing any objection to **processing** must be complied with.

14.5 The Trust is not however obliged to comply with a request where the **personal data** is required in relation to any claim or legal proceedings.

15 The Right to Rectification

15.1 If a **data subject** informs the Trust that **personal data** held about them by the Trust is inaccurate or incomplete then we will consider that request and provide a response within one month.

15.2 If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then we will inform the **data subject** within one month of their request that this is the case.

15.3 We may determine that any changes proposed by the **data subject** should not be made. If this is the case then we will explain to the **data subject** why this is the case. In those circumstances we will inform the **data subject** of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

16 The Right to Restrict Processing

16.1 **Data subjects** have a right to limit or suppress the **processing** of **personal data**. This means that the Trust can continue to hold the **personal data** but not do anything else with it.

16.2 The Trust may restrict the **processing** of **personal data**:

16.2.1 Where it is in the process of considering a request for **personal data** to be rectified (see above);

16.2.2 Where the Trust is in the process of considering an objection to processing by a **data subject**;

16.2.3 Where the **processing** is unlawful but the **data subject** has asked the Trust not to delete the **personal data**; and

16.2.4 Where the Trust no longer needs the **personal data** but the **data subject** has asked the Trust not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against the Trust.

16.3 If the Trust has shared the relevant **personal data** with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

16.4 The DPO must be consulted in relation to requests under this right.

17 **The Right to Be Forgotten**

17.1 **Data subjects** have a right to have **personal data** about them held by the Trust erased only in the following circumstances:

17.1.1 Where the **personal data** is no longer necessary for the purpose for which it was originally collected;

17.1.2 When a **data subject** withdraws consent – which will apply only where the Trust is relying on the individuals consent to the **processing** in the first place;

17.1.3 When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object;

17.1.4 Where the **processing** of the **personal data** is otherwise unlawful;

17.1.5 When it is necessary to erase the **personal data** to comply with a legal obligation; and

17.2 The Trust is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:

17.2.1 To exercise the right of freedom of expression or information;

17.2.2 To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;

17.2.3 For public health purposes in the public interest;

17.2.4 For archiving purposes in the public interest, research or statistical purposes; or

17.2.5 In relation to a legal claim.

17.3 If the Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

17.4 The DPO must be consulted in relation to requests under this right.

18 **Right to Data Portability**

18.1 In limited circumstances a **data subject** has a right to receive their **personal data** in a machine-readable format, and to have this transferred to another organisation.

18.2 If such a request is submitted, then the DPO must be consulted.

19 **Data security**

19.1 We will take appropriate security measures against unlawful or unauthorised processing of **personal data**, and against the accidental loss of, or damage to, **personal data**.

19.2 We will put in place procedures and technologies to maintain the security of all **personal data** from the point of collection to the point of destruction.

19.3 Security procedures include:

19.3.1 **Site Security.** Any unauthorised individuals seen in entry-controlled areas should be reported to the Executive Headteacher or a member of SLT. Doors to office spaces and teaching areas should be kept locked when unattended.

19.3.2 **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential). It is the individual responsibility of every employee to clear their desk or work area of any confidential information (which includes any information relating to an identifiable individual).

19.3.3 **Methods of disposal.** Paper documents should be destroyed in line with the Trust's retention schedule. Digital storage devices should be wiped and securely destroyed when they are no longer required by the Trust IT team.

19.3.4 **Equipment.** All employees must ensure that individual monitors do not show confidential information to passers-by and that they log off, or lock computers and mobile devices when they are left unattended.

19.3.5 **Working away from the academy premises – paper documents.** Employees are discouraged from removing paper documents containing confidential information from the academy sites. However, where this is necessary measures need to be put in place to ensure security of the documents. They must not be left in an unattended vehicle, not worked on in public and if taken home they must be secured in a locked cupboard until returned.

19.3.6 **Working away from the school premises – electronic working.**

Employees can access the school network securely from a remote device and when doing so the same security precautions much be taken. USB sticks are prohibited unless encrypted and documents must not be downloaded and stored in personal folders if they contain any personal data attributable to an individual student or employee.

19.3.7 **Document printing.** Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.

19.3.8 **Telephone, radio (where applicable) or discussions** in person relating to any confidential matter in respect of an identifiable individual must take place in private and not be overheard.

19.3.9 **Use of Online resources**: Where the school employs the use of mobile apps, cloud-based software or other online resources to aid the delivery of teaching and learning, appropriate checks concerning data protection compliance of suppliers will be undertaken prior to use. The Data Protection Officer should be consulted if the sharing pupil or staff data is necessary for the use of such resources (this can include

the registration and management of user accounts, or the supply of pupil data to support progress analysis and impact).

19.3.10 **Video Conferencing**: If videoconferencing technologies are used to support meetings or the delivery of blended/remote learning. The Headteacher should approve this use in the first instance. Staff should first consider any implications for the operation of school safeguarding practices when using video conferencing. Guidance is available for all staff on using video conferencing to support teaching and learning.

19.3.11 **Cyber Security:** Staff should not open any email attachments or click on embedded hyperlinks sent in emails from unrecognised senders. Suspicious emails should be reported immediately to the Trust IT team. If staff are concerned that the security of user accounts, passwords, or the access to work systems have been compromised, this should be reported immediately to the Trust IT team.

19.4 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

19.5 **Data Disposal**. The Trust recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All emails are retained for the period of two years only, unless messages contain personal data that requires a longer retention period. CCTV data is retained for one month.

All data held in any form of media shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or disposed of in accordance with the Trust retention schedule and guidelines published in the IRMS toolkit for academies.

Disposal of IT assets holding data shall be in compliance with ICO guidance:

https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf

20 Data Protection Impact Assessments

20.1 The Trust takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

20.2 In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or the way that we intend to do so.

20.3 The Trust will complete an assessment of any such proposed **processing** and has a template document which ensures that all relevant matters are considered.

20.4 The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

21 Disclosure and sharing of personal information

21.1 We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, and / or Education and Skills Funding Agency "ESFA", Ofsted, health authorities and professionals, Occupational Health, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

21.2 Staff should not share personal data with any external agencies, system providers or other individuals, unless this has first been authorised by the Executive Headteacher and, or the Data Protection Officer

21.3 The Trust will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.

21.4 In some circumstances we are required to share safeguarding information with relevant agencies. Please refer to our Child Protection Policy.

21.5 Further detail is provided in our Schedule of Processing Activities.

22 Data Processors

22.1 We contract with various organisations who provide services to the Trust. Where relevant these are named in the Privacy Notices we publish.

22.2 In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

22.3 **Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust. The Trust will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

22.4 Contracts with **data processors** will comply with Data Protection Legislation and contain explicit obligations on the **data processor** to ensure compliance with the Data Protection Legislation, and compliance with the rights of **Data Subjects**.

23 Images and Videos

23.1 Parents and others attending Trust and Academy events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. The Trust does not prohibit this as a matter of policy.

23.2 The Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Trust to prevent.

23.3 The Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

23.4 As a Trust we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils before allowing the use of images or videos of pupils for such purposes.

23.5 Whenever a pupil begins their attendance at the Academy they will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

24 CCTV

24.1 The Trust operates a CCTV system. Please refer to the Trust CCTV Policy.

25 Register of breaches

25.1 The Trust must maintain an accurate and up-to-date register of all Personal Data Breaches.

25.2 If anyone becomes aware of a Data Protection breach they must inform the Data Protection Officer immediately. A plan for managing Data Breaches will be made available to all staff.

26 Requests for information

26.1 Requests for information may take the following forms:

26.1.1 Requests for education records.

26.1.2 Freedom of information requests.

26.1.3 Subject access requests.

Where a person with parental responsibility requests information about a child's educational records, then requests should be submitted in writing to the Data Protection Officer at EBN Trust, C/O EBN Academy 2, 10 High Street, Birmingham, B35 7PR. Valid requests will be completed within 15 **school days**

26.2 If a person makes a request for information under the Freedom of Information Act, then the information should usually be provided unless there are some specific concerns about disclosing the information. Common concerns in the academy context may be that information relates to other people, is confidential or legally privileged. If a freedom of information request is made and there are any concerns about disclosing information, then the Data Protection Officer should be contacted. Requests should be submitted in writing to the Data Protection Officer at EBN Trust, C/O EBN Academy 2, 10 High Street, Birmingham, B35 7PR. Valid requests will be completed within 20 **Working (School) Days**

26.3 If a person makes a subject access request, then they are requesting the personal information that the academy has about them. There are exemptions to disclosing

some information but these are more limited as a person has a right to know what information is held on them. Requests should be submitted to the Data Protection Officer at either DPO@EBNFS.org or in writing to at EBN Trust, C/O EBN Academy 2, 10 High Street, Birmingham, B35 7PR. Requests can also be made verbally to the school office. Valid requests will be completed within 30 **Calendar Days**

27 **Changes to this policy**

We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

ANNEX

DEFINITIONS

Term	Definition
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our workforce (including Governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data

Workforce	Includes, any individual employed by Trust such as staff and those who volunteer in any capacity including Governors and/or Trustees/ Members/parent helpers.