Eaton Bray Academy

DATA PROTECTION POLICY

V0.3

Headteacher:	Mrs. S. Hounslow
Address:	School Lane Eaton Bray LU6 2DT
Tel No:	(01525) 220468
Email:	admin@eba.ec
Website:	www.eatonbrayacademy.co.uk

Eaton Bray Academy

Data Protection Policy

VERSION:	V0.3
VERSION DATE:	25th May 2018
AUTHOR:	Office Manager
REVIEWED BY:	Governing Body

AMENDMENT HISTORY

Issue	Author	Date	Description
V0.1(Draft)	SH	17/10/2012	Initial draft
V0.1	SH	30/09/2013	Formally approved by Governing Body
V0.2	SH	29/04/2015	Reviewed and no amendments made
V0.3	RM	25/05/2018	Reviewed and updated for GDPR

Introduction

Eaton Bray Academy recognises and accepts its responsibility as set out under the General Data Protection Regulation (GDPR) which came into force on 25th May 2018. The School, as a Data Controller, will take all reasonable steps to meet this responsibility and to promote good practice in the handling and use of personal information.

This policy statement applies to all School governors and employees, and individuals about whom the School processes personal information, as well as other partners and companies with which the School undertakes it business.

Mrs. S Hounslow
Headteacher

CONTENTS

1

1 Scope

Eaton Bray Academy needs to collect and use certain types of personal information about people with whom it deals in order to operate. These include current, past and prospective employees, pupils, parents, suppliers, clients, and others with whom it communicates. In addition, it may be required by law to share certain types of information about its staff and pupils with other organisations, for example the Department for Education, the Local Authority, other schools and educational bodies, health and welfare services.

This personal information must be dealt with properly, however it is collected, recorded and used - whether on paper, on a computer, or recorded on other material. The School will ensure that it treats personal information lawfully, correctly and in compliance with the General Data Protection Regulation (GDPR).

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how we comply with the core principles of the GDPR.

2 Legal framework

This policy has due regard to legislation, including:

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

This policy will be implemented in conjunction with the following school policies and documents, which are available to view on the school website:

- EBA E-Safeguarding Policy
- EBA Freedom of Information Policy
- EBA Data Breach Policy

- EBA Subject Access Request Policy
- EBA Confidentiality and Retention of Records Policy
- EBA Privacy Notice

3 DEFINITIONS

Data Controller: Any individual or organisation who controls personal data, in this instance the School.

Data Processor: The service provider/supplier who processes the data on behalf of the Data Controller, e.g. third parties with whom we share data in accordance with our legal obligation.

Personal Data: Information held on a relevant filing system, accessible record, manual filing systems or computerised record (as well as digital, audio or video equipment), which identifies living individuals. This extends to IP addresses, biometric data, mobile devices and website cookies.

Sensitive Personal Data: referred to in the GDPR as "special categories of personal data", this is data relating to an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life, sexual orientation.

Relevant Filing System: Also known as manual records i.e. a set of records which are organised by reference to the individual/their criteria and are structured in such a way as to make specific information readily accessible

Data Subject: An individual who is the subject of the personal data, for example, employees, pupils, parents etc.

Processing: Obtaining, recording or holding data or carrying out any operation on the data including organising, adapting, altering, retrieving, consulting, using, disclosing, disseminating, aligning, blocking, erasing or destroying the data.

Accessible Records: Any records which are kept by the Organisation as part of a statutory duty, eg pupil records.

4 Data Protection Principles

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and kept up-to-date; every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

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

5 Accountability

- Eaton Bray Academy will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

- The Academy will provide a comprehensive, clear and transparent Privacy Notice.
- Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to safeguarding.
- Internal records of processing activities (Data Audit/Log) will include the following:
  - Name and details of the Data Processor
  - Purpose(s) of the processing
  - Description of the categories of individuals and personal data
  - Retention schedules
  - Categories of recipients of personal data
  - Confirmation of technical and organisational security measures
  - Details of any transfers overseas including confirmation of the transfer mechanism safeguards in place

The trust will implement measures that meet the principles of "data protection by design and data protection by default", such as:

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

Data protection impact assessments will be used, where appropriate.

6 Data Protection Officer (DPO)

A DPO will be appointed in order to:

- Inform and advise the trust and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the trust's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

7 Lawful Processing

Under the GDPR, data can be lawfully processed under the following conditions:

- **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Eaton Bray Academy collect and use pupil information under the legal basis of **public task** as an educational setting/school with the delegated task of educating and safeguarding the children in our care and under a **legal obligation** which necessitates our school making statutory data returns to the Department for Education (DfE) and the our Local Authority.

The special categories of data have been collected through explicit **consent** from the data subject (or parent/legal guardian of the data subject for children under 13 years) in support of the specific purposes for which the data is being used in the education and safeguarding of pupils in our care.

For further information please see our Privacy Notice.

Where **consent** is required, e.g. for using children's photographs in school publications and on the school website, this must be a positive indication.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Where consent is given, a record will be kept documenting how and when consent was given.

Consent can be withdrawn at any time.

8 Privacy Notice

The Privacy Notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

The Privacy Notice will detail the following:

- The identity and contact details of the controller, and where applicable, the controller's representative and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- The retention period or criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
  - withdraw consent at any time.
  - report any concerns to a supervisory authority.

9 Data Subject Rights

Under GDPR data subjects (or the parent/carer of data subjects under the age of 13 years) have the following rights:

- Right to be informed
- Right to access their personal information
- Right to have inaccurate personal data rectified, blocked, erased or destroyed in certain circumstances

- Right to object to processing of personal data that is likely to cause, or is causing, damage or distress
- Right to restrict processing for the purpose of direct marketing
- Right to data portability
- Right to object to decisions being taken by automated means
- Right to claim compensation for damages caused by a breach of the Data Protection regulations

Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

The school is required to provide the individual with the data it holds on them within one calendar month. An extension of up to one calendar month can be granted if a school closure period is scheduled to occur during the initial one calendar month response time.

Please see our Subject Access Request Policy for further information.

Individuals are entitled to have any inaccurate or incomplete personal data rectified. Requests for rectification will usually be responded to within one month. An extension of up to one calendar month can be granted if a school closure period is scheduled to occur during the initial one calendar month response time.

Where it is determined by the controller that no action should be taken in response to a request for rectification, the trust will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent

- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- Where the personal data was unlawfully processed
- Where the personal data is required to be erased in order to comply with a legal obligation

The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

10 MONITORING

Eaton Bray Academy will act in accordance with the GDPR by adopting a "privacy by design" approach and implementing technical and organisational measures which demonstrate how we have considered and integrated data protection into processing activities.

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

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

A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

The trust will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the trust will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

11 Data Breaches

The term “personal data breach” refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Head will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their continued professional development training.

Please see the Data Breach Procedure Policy for more information.

12 Data Security

Paper records:

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital Data:

- Digital data is password-protected on a network drive that is regularly backed up off-site.

- All necessary members of staff and governors are provided with their own secure login for the school network, email system, MIS and other applications where personal data is stored.
- Staff and governors will use only their school email accounts and not their personal email for any school related business
- Staff and governors are aware of the need for complex (strong) passwords and are regularly prompted to change their passwords.
- Staff and governors will not share their passwords with others or save their passwords in web browsers
- Staff will ensure that computer screens are not positioned in such a way that they can be read from outside the room and will lock computer screens or log off when away from the computer.
- Staff will not store or hold pupil or staff data on any device not owned by the school or that forms part of part of the school network (eg, personal laptops or computers, mobile devices, cameras, memory sticks, cloud storage account)
- If a member of staff or of the governing body needs to use their own device for any school business (e.g. working from home), they must ensure that any documents downloaded are promptly and permanently deleted from the device.
- Where data is saved on a school owned removable storage or portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Confidential or sensitive information is not included in the body of an email if there are unsecure servers between the sender and the recipient.
- Email attachments containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- Circular emails to parents are sent via Parentmail or blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- All staff will sign and adhere to the Staff ICT Acceptable Use Policy (see E-Safeguarding Policy)

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices

under lock and key. The person taking the information from the trust premises accepts full responsibility for the security of the data.

Encrypted memory sticks will be issued by the school to those staff that require them. The following conditions apply:

- The encrypted memory sticks remain school property and should be return to school should the staff member leave.
- Users should not share their passwords with anyone else
- There will be a second password, recorded and stored securely and accessible only to approved staff, to enable school to access the data in the event that the staff member should forget their own password
- Data will be automatically deleted after six incorrect password attempts

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it
  - if being sent electronically a secure transfer system or encrypted email server is used.
  - If the document can only be sent by email it should be password protected
  - if being sent by post or courier it should be double bagged, the inside bag marked confidential/sensitive and recorded delivery should be used.
- That the individual or body that the data is being shared with can demonstrate that they are fully compliant with the GDPR.
- That who will receive the data has been outlined in a privacy notice.

Under no circumstances are visitors allowed access to confidential or personal information unless they have specific authorisation to do so. Visitors to areas of the school containing sensitive information are supervised at all times.

The physical security of the trust's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Eaton Bray Academy takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

13 Website and Blog

Eaton Bray Academy publishes a number of statutory and non-statutory documents on its website, including:

- Policies and procedures
- Annual reports
- Financial information

We will not publish any personal information, including photos, on our website or blog without the permission of the individual or their parent/guardian.

14 CCTV and Photography

Eaton Bray Academy understands that recording images of identifiable individuals constitutes processing personal information, so it is done in line with data protection principles.

- We notify all pupils, staff and visitors of the purpose for collecting CCTV images via notices throughout the school.
- Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
- All CCTV footage will be kept for six months for security purposes

If the school wishes to use images/video footage of pupils in a publication, such as the website, blog, prospectus, or recordings of school plays, we will ensure that permission has been granted for that particular usage.

15 Data Retention

Data will not be kept for longer than is necessary and unrequired data will be deleted as soon as practicable.

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

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

Please see our Confidentiality and Retention of Records Policy for further information.

16 DBS Data

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

Data provided by the DBS will never be duplicated.

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