EASTBURY COMMUNITY SCHOOL

DATA PROTECTION POLICY

If printed, copied or otherwise transferred from this website this document must be considered to be an uncontrolled copy.

Policy amendments may occur at any time and you should consult the Policies page on the website for the latest update.

Controlled Document

Document Name: Data Protection Policy

Document Version Number: Version 1

Author: Data Protection Enterprise, Data Protection Consultant

Authorised by: The Chair of Governors

Date: August 2018

Review Date: September 2019 or earlier where there is a change in the applicable law

Owner: Executive Headteacher

Version Control:

Version	Date	Author	Description of Change
1	25/07/18	Data Protection Enterprise www.dpenterprise.co.uk	New Policy

Contents:

1. INTRODUCTION

Eastbury Community School ("the School") is fully committed to compliance with the requirements of the General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018 (the DPA). The school will therefore, follow procedures which aim to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is processed fairly, lawfully and transparently.

The GDPR, the DPA and Article 8 of the Human Rights Act 1998, stress that the processing of personal data needs to strike a balance between the needs of the school to function effectively and efficiently and respect for the rights and freedoms of the individual. This policy sets out how the school intends to safeguard those rights and freedoms.

Obligations and responsibilities under the General Data Protection Regulations are not optional; **they are mandatory**. There can be harsh penalties, up to €20 million or 4% of global turnover for the preceding year (whichever is the greater) in relation to breaches of rights and obligations and up to €10 million or 2% of global turnover for the preceding year (whichever is the greater) imposed for non-compliance regarding Control and Mitigation.

The school will therefore, follow procedures that aim to ensure that all staff, pupils, parents, governors, visitors and any other person working for us who have access to any personal data held by or on behalf of the us is fully aware of, and abides by their duties and responsibilities under the General Data Protection Regulation and Data Protection Act.

All individuals permitted to access personal data in line with their work duties must agree to comply with this policy and agree to undertake any relevant training that may be appropriate to the role being undertaken.

As well as the school, any individual who knowingly or recklessly processes data without appropriate consent or proper authorisation, for purposes other than those for which it is intended or is deliberately acting outside of their recognised responsibilities may be subject to the school's disciplinary procedures, including dismissal where appropriate, and possible legal action liable to prosecution and possible criminal conviction under the Criminal Justice and Immigration Act 2008.

2. SCOPE

This policy applies to the collection and processing of all personal data held by the school, falling within the scope of the GDPR and the DPA in all formats including paper, electronic, audio and visual. It applies to all staff, governors, volunteers and contractors.

3. PERSONAL AND SPECIAL CATEGORY PERSONAL DATA

The GDPR and DPA provides conditions for the collection and processing of any personal data. It also makes a distinction between **personal data and 'special category' personal data**.

Personal data means any information relating to an identified or identifiable natural person ('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.

Special category personal data is defined as personal data consisting of information as to:

- racial or ethnic origin;
- political opinion;
- religious or other beliefs;
- trade union membership;
- physical or mental health or condition;
- sexual life or sexual orientation;
- genetics
- biometric data (where used for ID purposes)

Although there are clear distinctions between personal and special category data for the purposes of this policy the term *'personal data'* refers equally to *'special category data'* unless otherwise stated.

The GDPR and DPA rules for special category data do not apply to information about criminal allegations, proceedings, or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures.

4. PERSONAL DATA PROCESSED BY THE SCHOOL

The school processes personal data for many reasons to provide an education to its pupils. A description of the types of personal data processed and the purposes for processing are included in the school's privacy notices.

Personal data must be handled and dealt with in accordance with the GDPR and DPA and this policy. There are safeguards within the GDPR and DPA to ensure personal information is collected, recorded and used whether it is on paper, computer records or recorded by any other means.

The obligations outlined in this policy apply to everyone who has access to, holds copies of or processes personal data. This includes those who work at/from home or have remote or flexible patterns of working.

5. THE DATA CONTROLLER

The Dater Controller is the person who (either alone or jointly or in common with other persons) determines the purposes and manner for which personal data are or are to be processed. The Executive Headteacher is the Data Controller for the school.

6. ROLES AND RESPONSIBILITIES

6.1 Governing Board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

6.2 Data Protection Officer

The 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 school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the Information Commissioner's Office (ICO).

Our DPO is contactable via email at: dataprotection@eastburyschool.co.uk

6.3 Executive Headteacher

The Executive Headteacher acts as the representative of the data controller on a day-to-day basis.

6.4 All Staff

All Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy;
- Informing the school 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 you have concerns that this policy is not being followed
    - If you are unsure whether or not you have a lawful basis to use personal data in a particular way
    - If you need to rely on or capture consent, deal with the rights of the data subjects or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whether you are engaging in a new activity that may affect the privacy rights of individuals
    - If you need help with any contracts or sharing personal data with third parties

7. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with 6 principles of good practice. These principles are legally enforceable and can be summarised as follows:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Obtained 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;

3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely 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;
6. 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. In accordance with the rights of data subjects under the GDPR and DPA.

8. FAIR PROCESSING

In meeting any obligation to ensure that processing of information is fair, due consideration will be given to the adoption of any recognised standards or advice to provide individuals with such information as is necessary to ensure that they are likely to understand: -

a) The purposes for which their personal data are to be processed;
b) The likely consequences of such processing and;
c) Whether particular disclosures can be reasonably envisaged

9. NOTIFICATION

The national body for the supervision of GDPR is the Information Commissioners' Office to whom the Executive Headteacher notifies his/her purposes for processing personal data.

This notification process serves to provide transparency and openness about the processing of personal data. It is a fundamental principle of the GDPR that the public should know or be able to find out who is carrying out the processing of personal data and for what purpose.

A copy of the school's notification details is available on the Information Commissioner's website www.ico.org.uk

10. INDIVIDUALS' RIGHTS

The school recognises that access to personal data held about an individual is a fundamental right provided in the Act. These rights include: -

- The right to be informed
- The right of access to personal information
- The right to request rectification
- The right to request erasure
- The right to restrict processing in certain circumstances
- The right to data portability
- The right to object to processing
- Rights to automated decision making including profiling

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil.

This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

The school will ensure that all requests from individuals to access their personal data are dealt with as quickly as possible and within the 15 school-day timescale allowed in the legislation, as long as the data subject meets the requirements set out in this policy. To minimise delays and unnecessary work all requests from data subjects must:

- Be made in writing (paper or email) to dataprotection@eastburyschool.co.uk
- Be accompanied by adequate proof of the identity of the data subject where required and, where applicable, the written authorisation of the data subject (if the request is being made on their behalf by a legal or lawfully appointed representative or, authorised agent).
- Specify clearly and simply the information required.
- Give adequate information to enable the requested data to be located
- Make it clear where the response should be sent.

The Data Protection Officer must be informed of any request to action against one or more of these rights.

The Act allows exemptions from providing information to individuals making a subject access request, and non-disclosure of information, in specific and limited circumstances.

The school will normally apply the exemptions and the non-disclosure of information rules, unless it is satisfied that it is appropriate or reasonable not to do so and, in any event, will always do so in circumstances where it is deemed necessary to the effective operation of the school, for the prevention and detection of crime, to protect the individual or is required by law.

If a data subject remains dissatisfied with a response received, they may ask for the matter to be reviewed, or, in the case of an employee through the school's grievance process.

Ultimately if a data subject continues to be dissatisfied, she/he has the right to ask the Information Commissioner's Office (ICO) to carry out an assessment of their case and/or pursue a legal remedy.

11. LEGAL REQUIREMENTS

The school may be required to disclose personal data by a court order, or to comply with other legal requirements including the prevention or detection of crime, apprehension of an offender or gathering of taxation.

External agencies or companies contracted to undertake processing of personal data on behalf of the school must demonstrate, via a written agreement, that personal information belonging to the school will be handled in compliance with the GDPR and DPA and that it has the necessary technical and organisational security measures in place to ensure this.

Any sharing of the school data with external partners for the purpose of service provision must comply with all statutory requirements.

The school will follow relevant guidance issued by the Government and the ICO for users of CCTV and similar surveillance equipment monitoring spaces to which the public, residents, service users and employees have access and will also strive to ensure that partner organisations involved in joint or multi-agency initiatives seek to do the same. The school reserves the right to monitor telephone calls, email and internet access in compliance with relevant legislation. This will be handled in line with guidance issued by the ICO.

The legal basis for this policy is the GDPR and DPA which provides the legal parameters for the processing of personal data. However, compliance with other legislation, Codes of Practice, policies and guidance also has relevance, such as;-

- The Freedom of Information Act 2000
- The Computer Misuse Ace 1990
- The Crime and Disorder Act 1998
- Human Rights Act 1998

12. DATA SECURITY

The school will process personal data in accordance with its Information Security Policy (and other related Policies and Procedures). To ensure the security of personal data, the school has appropriate physical, technical and organisational measures in place. Employees are required to comply with the Information Security Policy.

The GDPR and DPA requires that appropriate technical and organisational measures shall be taken to protect data against:

- Unauthorised access;
- Unauthorised or unlawful processing;
- Accidental loss, destruction, or damage

Appropriate technical and organisational security measures will include:

- using and developing technological solutions to ensure compliance with the data protection principles
- using and developing physical measures to protect school assets
- ensuring the reliability of any persons who have access to school information
- reporting and investigating security breaches

These obligations include the need to consider the nature of the data to be protected and the harm that might arise from such unauthorised or unlawful processing or accidental loss, destruction, or damage.

All printout material, magnetic tape, diskettes, CD's or DVD's, manual files, hand written notes etc, which contain personal data and are no longer required, will be treated as confidential waste, and disposed of securely.

Where processing of school data is to be carried out by a third party on behalf of the school, the Headteacher must ensure that the third party provides sufficient guarantees in respect of the technical and organisation measures governing the processing to be undertaken.

13. SHARING PERSONAL DATA

We will not normally share personal data with anyone else, but may do so where:

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

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

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

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

14. BIOMETRIC RECOGNITION SYSTEMS

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash) we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

15. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Further information about the school's CCTV system can be found in our CCTV policy on the website.

16. DATA PROTECTION BY DESIGN AND DEFAULT

The school will use a Data Privacy Impact Assessment (DPIA) toolkit to evaluate all new computer systems to help it determine how data protection compliance can be assured. In addition, all existing systems will be subject to periodic assessment.

DPIA toolkits provide a step-by-step approach to evaluate the test proposed, new or existing information systems for compliance with the legislation. The DPIA process helps to identify weaknesses or risks to data losses or breaches and consider action that needs to be taken to ensure compliance where such compliance is not yet achieved. DPIA applies equally to paper as well as electronic data holding systems.

The Data Protection Officer **must** be consulted when carrying out a data protection impact assessment.

17. PERSONAL DATA BREACHES

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in our Security Incident and Data Breach Policy.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person

- The theft of a school or personal electronic device containing non-encrypted personal data about pupils
- Accidental disclosure of personal data to another person or organisation
- Inappropriate access to or use of personal data
- The theft of personal information, either paper based or electronic
- Accidental loss of personal data
- Information that has not arrived at its destination
- Fraudulent acquisition of personal data (Blaggers)

18. TRAINING AND AWARENESS

Data Protection training and awareness is crucial so that all staff understand their responsibilities relating to data protection and the use of personal data. Failure to comply with the GDPR, DPA and the principles could lead to serious problems, and in some cases may result in significant fines or criminal prosecution.

It is the school's policy that all employees including managers and governors are required to complete the applicable training course annually. This includes employees that do not have internet or email access. Line managers will be responsible for ensuring that staff without internet or email access receive appropriate training.

19. OUR COMMITMENT TO DATA PROTECTION

The Executive Head of Eastbury Community School will be accountable for ensuring compliance with this policy.

The school will ensure that individuals handling personal information will be trained to an appropriate level in the use and control of personal data.

The school have implemented a process to ensure all staff handling personal information know when and how to report any actual or suspected data breach(es), and that appropriately trained staff manage these breaches correctly, lawfully and in a timely manner.

The school will monitor and review its processing activities to ensure these are consistent with the principles of the GDPR and DPA and will ensure that its notification is kept up-to-date.

The school will ensure that any new or altered processing identifies and assesses the impact on a data subject's privacy as a result of any processing of their personal data, and that appropriate Privacy Notices are maintained to inform data-subjects of how their data will be used.

The school will review and supplement this policy to ensure it remains consistent with the Law and any compliance advice and Codes of Practice issued from time to time by the ICO.

20. POLICY REVIEW

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed annually. In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.

19. LINKS WITH OTHER POLICIES

This data protection policy is linked to our:

- Freedom of information Policy
- Security Incident and Data Breach Policy

- CCTV Policy
- Data Sharing Policy
- Data Privacy Impact Assessment Policy
- Acceptable use policy
- Safe guarding policy
- GDPR Privacy Notices

The ICO also provides a free helpdesk that can be used by anyone and a website containing a large range of resources and guidance on all aspects of Information Law for use by organisations and the public. See www.ico.org.uk