Data Protection Policy (GDPR) Ernest Bevin Academy The best in everyone™ Part of United Learning	
Strategic Aims **This policy aims to:** • Outline how and why Ernest Bevin Academy collects personal information and what we do with that information.	
Responsibility: Wandsworth DPO	**Date Approved:** Autumn 2023
Approved by: Principal	**Review Date:** Autumn 2024
Monitored by: Head of Network Services and Learning Resources	**Links to other Policies:** Privacy Notice for Pupils Privacy Notice for School Workforce Remote Provision Policy Online Safety Policy

Introduction

This policy meets the requirements of the General Data Protection Regulation (GDPR) and provisions of the Data Protection Act (DPA) 2018. It is based on guidance published by the Information Commissioner's Office (ICO) for the GDPR, the ICO's code of practice for subject access requests and the ICO's code of practice for the use of surveillance cameras and personal data. Overall security policy for data is determined by the Principal / Governing Body / Senior Management and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. This document applies to all data, regardless of the format, be it paper or electronic.

Any queries or concerns about security of data in the Academy should in the first instance be referred to the Data Protection Officer (DPO)

Responsibilities

This document applies to all staff employed by Ernest Bevin Academy, and to all organisations or individuals working on and with Ernest Bevin Academy behalf. Any individual/s who fail to comply with this policy may face disciplinary action. We will ensure ALL the Academy stakeholders sign an 'Acceptable User Policy'

Data Controller

Ernest Bevin Academy processes personal data and information relating to all parents, students, staff, governors, and other individuals. Therefore, Ernest Bevin Academy is a data controller.

Data Protection Officer (DPO)

The DPO is responsible for overseeing the implementation of this policy, monitoring Ernest Bevin Academy compliance with data protection law, and creating guidelines and policies when and where needed. The DPO will provide an annual report of his/her activities directly to the Governing Body where relevant. Gary Hipple will be EBC's Data Protection Officer

with responsibility for data protection compliance. The DPO is also the first point of contact for individuals whose data the Academy processes, and the ICO.

Governors
The Governing body has overall responsibility for ensuring that Ernest Bevin Academy complies with all relevant data protection obligations.

Principal
The Principal is the Senior Information Risk Officer (SIRO).

Staff
Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from individuals who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as a disciplinary matter, and serious breaches could lead to dismissal.

All Staff employed by Ernest Bevin Academy are responsible for:

- Storing, processing and collecting any personal data in accordance with the policy outlined in this document
- Informing the Academy of any changes to their personal data/details, for example, a change of phone number or change of address
- Informing the Academy on the loss or misplacement of their ID cards.
- Contacting the DPO under the following circumstances:
    - If they have any questions about the usage and operation of this policy, data protection law, storing personal data
    - If they have questions on how to keep personal data secure
    - If they have any concerns about this policy not being followed
    - If they are unsure on whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or get consent, draft a privacy notice, deal with data protection rights invoked by any individual/s, or transfer personal data outside the European Economic Area
    - If there has been or a risk of a data breach
    - Whenever there is a process that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing of personal data with third parties

Ernest Bevin Academy outlines and emphasizes the key points below:

- **We ensure that staff know to immediately report any queries or concerns about security of data or any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, to the Head of Network and Learning Resources.**

- Staff are clear who the key contact(s) for key Academy information are (the Information Asset Owners). We have listed the information and information asset owners in a spreadsheet document
- All staff are **DBS** checked and records are held in **SIMS.**
- All staff are provided with ID cards. Staff are required to register their presence on the premises as soon as they arrive or leave the site using the InVentry card readers on site. This data is collected for Health and Safety purposes.
- We have approved educational web filtering across our wired and wireless networks.
- We also have **LGFL** as an additional layer of monitoring software across our network system.
- We monitor Academy e-mails / blogs / online platforms, etc, to ensure compliance with the 'Acceptable Use Policy'. As well as monitoring usage, we may also monitor content of e-mails / blogs / etc.
- We follow Wandsworth guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- All staff have their own unique username and private passwords to access Academy systems. Staff are responsible for keeping their passwords private.
- We encourage staff to use **STRONG** passwords for access into our MIS system.
- We require staff to change their passwords twice a year.
- We require that any personal/sensitive material must be encrypted if the material is to be removed from the Academy, and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- Staff who set up usernames and passwords for e-mail, network access, other online services work within the approved system and follow the security processes required by those systems.
- We ask staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which need no longer be stored.

All employed staff by EBC must take every precaution to ensure that data is kept secure and used appropriately. These are the steps to follow:

- **Never** share usernames or passwords.
- **Don't** write down your passwords.
- **Don't** share your ID card with any third party.
- **Don't** use your personal email for work.
- **Avoid** using personal devices for work wherever possible.
- **Do not** use any third party cloud storage service
- **Don't** use Academy ICT equipment or systems for non-Academy activities.
- **Don't** install any hardware or software on a Academy device without authorisation

from the Network and Learning Resources.

- **Don't** use USB sticks to store or transfer unencrypted personal data.
- **Never** store children's personal data, including photos/videos, on a phone/other personal device.
- **Do not** print personal data. If any copies exist, destroy these when you no longer need it.
- **Do not** carry printed copies of personal data between Academy sites or taking it home
- **Don't** import children's personal data into any programmes or apps, without authorisation the Network and Learning Resource.
- **Don't** take or post photos or videos of children, with their full names, in a publication or online (website, social media), unless you are sure that explicit parental consent has been obtained by Ernest Bevin Academy.

All staff are provided with data protection training. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Academy policies make it necessary.

Data protection principles

GDPR is based on data protection principles that Ernest Bevin Academy must comply with. The data protection principles outline that all personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Accurate and, where necessary, kept up to date
- Collected for specified, explicit and legitimate purposes
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

Collecting of personal data

- Ernest Bevin Academy will only collect personal data for specified and legitimate reasons. These reasons are clearly outlined to the individuals when we first collect their data.
- If Ernest Bevin Academy wants to use personal data for reasons other than those given when we first obtained it, we will inform all individuals involved before we do so, and seek consent where and when necessary.
- All staff must only process personal data when and where necessary.
- When staff no longer need the personal data that is held, staff must ensure it is deleted.
- All records containing personal information should be made illegible and properly

disposed of. Paper records should be shredded. See the Network Services team on how to properly dispose of physical devices holding any data.

Sharing of personal data

Ernest Bevin Academy will not normally share personal data, but may do so where:

- There is an issue with a student or parent/carer that puts the safety of our student, staff or parents/ carers at risk
- We need to liaise with external bodies – we will seek consent where appropriate before doingso

Any of our suppliers or contractors need data to enable us to provide services to our staff and students – 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 students 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.

Photography and videos

As part of Ernest Bevin Academy activities, we may take photographs and record images of individuals within Ernest Bevin Academy. Some examples of how images or videos may be used within our premises include:

- As part of a learning activity; e.g. a teacher photographing a student at work and then sharing the pictures in the classroom, allowing them to see work and

make improvements.

- Plasma screens, banners, displays & photos around Academy (internal buildings)
- For presentation purposes around the Academy; e.g. in wall displays or slideshows that celebrate student's work and achievements (student's name will not be used beside a photograph of them)
- As part of a recorded lesson observation; e.g. teachers using video to help them review and evaluate their practice, and discuss their lesson with other staff in order to develop their teaching.

Ernest Bevin Academy will ensure written consent is obtained from parent/carer for photographs and videos to be taken of students for marketing and promotional materials. Ernest Bevin Academy will clearly explain how any photographs/videos will be used to all parties. Areas where images/videos may appear externally include:

- Academy website
- Academy prospectus & Sixth Form Prospectus
- Open Morning and Evening presentations by the Principal, banners outside Academy, leaflets & fliers
- Advertisements for the Academy to appear in newspapers, magazines, buses, posters, presentations, digital screens & on social media
- Wandsworth Council 'Choose a Wandsworth Secondary School' booklet
- Academy publications including Academy Calendar, Guide for Families that are distributed to all
- Academy Social media sites including Twitter, Facebook, Linked In
- In a presentation about Ernest Bevin Academy and its work, in order to share its good practice with other schools
- In the media; e.g. if a newspaper photographer or television film crew attend an event.

Consent can be refused/withdrawn. If consent is withdrawn, Ernest Bevin Academy will delete data and not distribute it further. Photos displayed internally will be removed within a reasonable timescale (unless we are notified otherwise)

When using images/video, Ernest Bevin Academy will not include any other personal data about the student.

CCTV

CCTV is used in various locations around Ernest Bevin Academy premises for safety purposes. We will adhere to the ICO's code of practice for the use of CCTV. While Ernest Bevin Academy does not need to ask individuals' permission to use CCTV, we make it clear where individuals are being recorded. Security cameras are clearly visible. Any enquiries about Ernest Bevin Academy CCTV system should be directed to the Principal. The CCTV

system is monitored during working hours.

Subject access requests

All individuals have a right to make a 'subject access request' to gain access to personal information that the Academy holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, is being, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:
    - Name of individual
    - Correspondence address
    - Contact number and email address
    - Details of the information requested
- If staff receive a subject access request they must immediately forward it to the DPO.

Responding to a request

When responding to requests, the

Academy

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond within 72 hours within term time only
- Will try to provide the information free of charge

Ernest Bevin Academy will not disclose information if it:

- May cause serious harm to the physical/mental health of the student or individual
- Will reveal that the student is at risk of abuse, where the disclosure of information will not be in the student's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the student

If the request is excessive or unnecessary, Ernest Bevin Academy holds the right to refuse to act on it, or to charge a fee which takes into account administrative costs. A request will be

deemed to be excessive or unnecessary if it is repetitive. If Ernest Bevin Academy refuses a request, we will inform the individual why.

Student request

Personal data about a student belongs to that individual student over the age of 13, not the student's parent/carer. For a parent or carer to make a subject access request on behalf of the student, the student must either be unable to understand their rights and the implications of a subject access request, or have given said parent/carer their consent. Students below the age of 12 are not regarded to be mature enough to understand their rights and the implications of a subject access request.

Other data protection rights

Individuals also have the right to receive information when we are collecting data, and how we use and process data. Individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask the Academy to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Data security

Ernest Bevin Academy will protect any and all personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. This includes:

- Paper records and portable devices (i.e. laptops and hard drives) that contain personal data are kept under lock and key when not being used
- Paper containing confidential data must not be left on office and classroom desks, on

staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access

- Where personal information needs to be taken off site, staff must sign it in and out from the Administration Office
- Passwords that are at least 7 characters long containing letters and numbers are used to access Ernest Bevin Academy computers, laptops and other electronic devices.
- Staff and students are reminded to change their passwords twice a year
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff or Governors who store personal information on their personal devices are expected to follow the same security procedures as for Academy-owned equipment (see our online safety policy for more information).
- Where we need to share personal data with a third party, the Academy will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

Disposal

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will corrected or be disposed of securely. For example, Ernest Bevin Academy will shred paper-based records, and overwrite or delete electronic files. Ernest Bevin Academy may also use a third party to safely dispose of records on the Academy behalf, where the Academy will require said party to provide sufficient guarantees that it complies with data protection law.

Data breaches

Ernest Bevin Academy will make all reasonable changes to ensure that there are no data breaches. In the event of a suspected data breach, we will follow the correct procedures. Ernest Bevin Academy will report any data breach to the ICO when deemed appropriate. Such breaches may include, but not limited to:

A non-anonymised dataset being published on the Academy website which shows the exam results of students

Safeguarding information being made available to an unauthorised person

The theft of a Academy laptop containing non-encrypted personal data about students

Monitoring

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill

receives Royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the full Governing Body.

Terms and Definitions	
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: Name (including initials) Photograph Identification number Location data Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: Racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership Genetics Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes Health – physical or mental Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.