ESPRIT Data Protection and Privacy Notice Policy

Full Governing Body agree to adopt this policy September 2018 and agree next review date of July 2019.

Contents

1. Aims

ESPRIT Multi Academy Trust aims to ensure that all personal data collected about staff, pupils, parents, members, trustees, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018, it is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition , this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • 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.

4. Roles and responsibilities

This policy applies to **all staff** employed by the Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

4.1 The Trust Board

The Trust Board has overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

4.2 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 report to the Trustee Board on their activities directly and where relevant report to the board their advice and recommendations on academy data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is Lesley Walter and is contactable via email on enquire@espritmat.org

4.3 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Academy of any changes to their personal data , such as change of address, change of name
- 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 they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there is a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals

- If they need help with any contracts or sharing personal data with third parties

5. Data Protection Principles

The GDPR is based on data protection principles that our Trust must comply with.
The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- 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

This policy sets out how the Trust aims to comply with these principles.

6. Collecting personal data

6.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of the 6 'lawful bases' (legal reasons) to do so under data protection law.

- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g to protect someone's life
- The data needs to be processed so that the Trust, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for **legitimate interests** of the Trust or a third party (provided the rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventative services).

6.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's toolkit for schools.

7. 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 or pupils 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.

8. Privacy/fair processing notice

8.1 Pupils and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the Trust is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on pupil characteristics, such as ethnic group or special education needs
- Exclusion information
- Details of any medical conditions

We only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so.

We are required, by law, to pass certain information about pupils to specified external bodies, such as our local authority, the Department for Education, Education Skills Funding Agency, so that they are able to meet their statutory obligations.

8.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our Trust. The purpose of processing this data is to assist in the running of the school, including to:

- Enable individuals to be paid
- Facilitate safe recruitment

- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Dates of birth
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority, the Department for Education and the Education Skills Funding Agency, so that they are able to meet their statutory obligations.

9. Subject access requests and other rights of individuals

Individuals have a right to make a 'subject access request' to gain access to personal information. 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, 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

Recital 59 of the GDPR recommends that we provide means for requests to be made electronically, especially where personal data are processed by electronic means. We therefore invite you to complete Appendix 3 and return to the Data Protection Officer. It 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.

You are entitled to submit subject access requests all year round, but please bear in mind that it may be necessary for us to extend the response period when requests are submitted over the summer holidays. This is in accordance with article 12(3) of the GDPR, and will be the case where the request is complex – for example, where we need multiple staff to collect the data.

9.1 Parental requests to see the educational record

Parents of pupils at this Trust do not have an automatic right to access their child's educational record. The Trust will decide on a case-by-case basis whether to grant such requests, and we will bear in mind guidance issued from time to time from the Information Commissioner's Office (the organisation that upholds information rights). Subject access requests for all or part of the pupil's educational record will be provided within 15 school days if the subject access request has been successful.

When responding to requests, we:

- May ask the individual for further identification
- May contact the individual via phone to confirm the request was made

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee, which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.2 Other data protections rights of the individual

In addition to the right to the above, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us 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.

10. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our Trust.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school brochures, magazines and newsletters
- Online on our school website or social media pages
- Outside of school by external agencies such as the school photographer, newspapers, campaigns

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

11. CCTV

We use CCTV in various locations around the Trust to ensure it remains safe. We will adhere to the ICO's code of practice. For further information on how and where we use CCTV please see our CCTV policy available on the website (currently under review)

12. Data Security and Storage of records

Paper based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept secure

Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access.

Staff when using electronic devices that contain personal information will lock their devices if left unattended for any length of time.

Where personal information is taken off site (in paper or electronic form), staff must ensure it is kept securely and following GDPR requirements.

Encryption software is used to protect all portable devices including laptops. Staff are not to use usb devices for school-based work.

Staff and Governing bodies who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment. (Need to list other appropriate policies here that link with Data protection –eg ICT policy/acceptable use agreement/acceptable use policy)

Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

13. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred paper based records, and

overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that is complies with data protection law.

14. Personal data breaches

The Trust 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 appendix 1

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a Trust 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 Trust laptop contained non-encrypted personal data about pupils.

15. Training

All staff, Members, Trustees and Governors are provided with data protection training as part of their induction process.

Data protection will also form part of the continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.

16. 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 received royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the Bill that affect our Trusts practice. Otherwise, or from then on, this policy will be reviewed annually and shared with the full governing board.

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO

- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people

- The DPO will alert the Executive Principal and the Academy Prinicpal in the first instance

- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

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

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

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust's secure document store.

- Where the ICO must be notified, the DPO will do this via the https://ico.org.uk/for-'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

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

APPENDIX 2 – Privacy Notice

Privacy notice for parents/carers.

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils**.

We, ESPRIT Multi Academy Trust, are the 'data controller' for the purposes of data protection law.

For the most up to date copies of our Privacy Notices, please visit either the Trust website or the individual Academies website.

2. Privacy notice for staff

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

We, ESPRIT Multi Academy Trust are the 'data controller' for the purposes of data protection law.

For the most up to date copies of our Privacy Notices, please visit either the Trust website or the individual Academies website.

Appendix 3

[Insert date]

insert your name and address

Re: subject access request

Dear *insert the name of your data protection officer,*

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

Name	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible*

If you need any more information from me, please let me know as soon as possible.

Please bear in mind that under the GDPR you cannot charge a free to provide this information, and in most cases, you must supply me with the information within 1 month.

Yours sincerely,

Name