Data Protection Policy

Introduction

The Teaching School Hubs Council aims to ensure that all personal data collected is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) 2018. Whilst each Teaching School Hub comes under the legal entity of the Multi Academy Trust they are part of, this overarching data protection policy has been produced.

Each Teaching School Hub provides professional development for teachers, and each one has a lead Trust who delivers the activities offered by the hub. The Data Protection Officer for our lead school is **Mark Allday: Assistant Headteacher, Sandringham School.**

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

Legislation and guidance

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

The regulation provides a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed, retained, deleted or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration and disclosure.

Definitions

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 undertaken relating 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.

Our Hub as a Controller/Processor

Our Teaching School Hub acts as both a processor and a controller, depending on the data in question. To see how we act in regard to a specific type of personal data, please request to view our data asset register.

Roles and responsibilities

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

Data Protection Principles

The GDPR is based on data protection principles that our organisation 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 organisation aims to comply with these principles.

Collecting personal data

Lawfulness, fairness, and transparency

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

- The data needs to be processed so that the organisation can fulfil a contract with the individual, or the individual has asked the organisation to take specific steps before entering into a contract
- The data needs to be processed so that the organisation 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 organisation, 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 the legitimate interests of the organisation or a third party (provided the individual's rights and freedoms are not overridden)
- The individual has freely given clear consent. Where the legal basis for processing is consent, for example direct marketing, you can withdraw your consent at any time, and we will cease to process the information further. Consent must be given on an opt-in basis, and it must be made clear at the point of giving consent that you can withdraw consent freely.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in article 9 of the GDPR and Data Protection Act 2018.

Our organisation will ensure that personal data is only handled in ways that would be reasonable expected, and not used in a way which may cause adverse effects on the subject.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Limitation, minimisation, and accuracy

We will only collect personal data for specific, explicit, and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. We will take steps to ensure that the personal data we collect and hold is accurate.

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 Records Management and Retention Schedule of the Trust overseeing the hub.

Sharing personal data

We may share your information with the following:

- Teaching Schools Hub delivery partners e.g. Trusts.
- Lead Providers
- Appropriate Body Assessors
- Other departments within the Teaching School Hub
- Department for Education
- Local authorities
- Third party consultants*
- ITT providers

*We ensure that all third parties that we share your data with are compliant with GDPR regulations and have appropriate policies and procedures in place.

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

Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the organisation 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, 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 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 Director of the Teaching School Hub.** It is important to note that subject access requests can be submitted verbally or through written means.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information 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.

Other data protection rights of the individual

In addition to the right to make a subject access request and to receive information when we are collecting their data about how we use and process it, 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 Director of the Teaching School Hub.**

Photographs and videos

On occasions we may take photographs or videos at events and we will use consent as the lawful basis to do this. 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.

Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Only process personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Integrate data protection into internal documents including this policy, any related policies and privacy notices
- Regularly train members of staff on GDPR legislation, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conduct reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our organisation and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left anywhere else where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access computers, laptops, and other electronic devices. Staff are required to change their passwords at regular intervals.
- Two factor authentication is used where possible
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff should not store personal information on their personal devices

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 or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on our behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with GDPR regulation.

Personal data breaches

The organisation 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 A.

Training

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

Appendix A

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

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

So, a data breach has occurred if personal data has been lost, stolen, destroyed (accidentally or in error), altered (accidentally or in error), disclosed accidentally or in circumstances where it should not have been or otherwise made available to unauthorised people.

Step 1: On finding or having caused a data breach, staff members or third-party data processors must notify the person responsible for data protection immediately.

Step 2: The point of contact must notify the Data Protection Officer immediately when notified of a breach.

Step 3: The organisation will take all reasonable steps to contain the breach and minimise its effects as far as possible, requesting action from staff members and any third-party data processors that may be required.

- Can the data be retrieved or safely deleted/destroyed by any unintended recipient(s)?
- Are we certain we have identified all the data that was lost/mistakenly disclosed or altered etc?

Step 4: At the earliest possible time, the organisation will assess the potential consequences of the breach. The organisation should consider;

- How could it affect the data subject(s) involved?
- How serious will these effects be for the data subjects?
- How likely is it that the data subjects could be affected in this way(s)?

Step 5: The organisation must decide whether or not the breach must be reported to the ICO. Breaches must be considered on a case-by-case basis; however, a breach must be reported to the ICO if it is likely to result in any physical, material or non-material damage such as;

- loss of control over their personal data
- limitation of their rights
- discrimination
- identity theft or fraud
- financial loss
- unauthorised reversal of pseudonymization
- damage to reputation
- or any other significant economic or social disadvantage to the individual(s) concerned

If the breach is likely to affect anybody in any of the ways described above, and cannot be successfully contained or rectified, it must be reported to the ICO.

Step 6: The organisation will document the decision taken as to whether or not the ICO are notified of the breach. The organisation should keep a record of this decision in case it is challenged at a later date by any of the individuals involved or by the ICO. The organisation should keep a record of breaches whether or not they are reported to the ICO. This record should include:

- A description of the breach and how it occurred
- Details of the data involved
- A description of the potential consequences of the breach
- Details of how likely it is any individuals could be affected
- A description of measures taken to contain or rectify the breach
- Actions taken to avoid any repeat of errors that lead to the breach

Step 8: In cases where the breach must be reported to the ICO, the organisation must do so within 72 hours of becoming aware of the breach. Such breaches are reported via the relevant page on the ICO's website.

Step 9: The organisation must decide whether or not the individual's affected by the breach must be notified. Again, the potential risks to any affected individuals (described in Step 5), the severity of any affects and the likelihood of them being affected must guide this decision-making process. If there is a high risk the organisation will notify, in writing, all potentially affected individuals. This notification will include:

- Contact details for the point of contact
- A description of how the breach occurred and the data involved
- A description of the measures taken to contain or rectify the breach
- Any advice it is possible to provide in terms of how the individuals could be affected

Step 10: The organisation must ensure records of breaches and decisions taken relating to them are stored and accessible in the event of any subsequent investigation by the organisation or the ICO.