DATA PROTECTION POLICY

Equa Multi Academy Trust issues this policy to meet the requirements incumbent upon it under The Data Protection Act 2018 for the handling of personal data in the role of controller. If appropriate it can also be used for the control and release of data under the Freedom of Information Act 2000.

Policy Lead	**CEO**
Committee	**Resources**
Adopted by Trust Board	**March 2019**
Last amended	
Last Review	**May 2023**
For Review	**Biannually**

Data Protection Policy

1. Introduction

Equa Multi Academy Trust issues this policy to meet the requirements incumbent upon it them under The Data Protection Act 2018 for the handling of personal data in the role of controller. If appropriate it can also be used for the control and release of data under the Freedom of Information Act 2000.

2. Scope

This policy applies to all employees of Equa MAT including contract, agency and temporary staff, volunteers and employees of partner organisations working for Equa MAT.

3. Legal Principles

In execution of this policy Equa MAT will comply with the data protection principles of the GDPR specified in Article 5. These are that personal data be:

a) processed **lawfully, fairly and in a transparent manner** in relation to individuals;

b) collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;

d) **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) 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 law in order to safeguard the rights and freedoms of individuals;

f) 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.

Equa MAT will adopt the appropriate technological and organisational measures to ensure compliance with the Data Protection Principles by carrying out the necessary procedures. The concept of *data protection by design* will be a guiding principle in achieving the security of individual's data protection rights.

In all aspects of our work we will ensure that the rights of the data subject are protected by all practicable measures associated with the conduct of our work. The rights of the data subject as defined in law are;

a) The Right to be informed in a clear, concise and transparent manner
b) The Right of access
c) The Right to rectification
d) The Right to erasure
e) The Right to restrict processing
f) The Right to data portability
g) The Right to object
h) Rights related to automated decision making

4. Special Categories of Data

The law puts in place extra protections for special category data and criminal convictions because of their sensitivity.

The categories of data which are considered "special" are personal data revealing an individual's:

a) racial or ethnic origin
b) political opinions
c) religious or philosophical beliefs
d) trade union membership
e) genetic data
f) biometric data for the purpose of uniquely identifying a natural person
g) data concerning health; or
h) data concerning a natural person's sex life or sexual orientation.

5. Legal Basis for processing sensitive data

In addition to the legal basis to process personal data, special categories of personal data also require an additional legal basis for processing under Article 9 of the GDPR. These grounds are as follows:

a) The individual has given **explicit consent** to the processing of those personal data for one or more specified purposes.

b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights under **employment, health and social security and social protection law and research**; a full list can be found in Schedule 1 Part 1 of the Data Protection Act 2018.
Health or social care purposes includes the following purposes-

i. Preventative or occupational medicine
ii The assessment of the working capacity of the employee

c) Processing is necessary to protect the **vital interests** of the individual or of another natural person where the individual is physically or legally incapable of giving consent

d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a **foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim** and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the individuals concerned.

e) Processing relates to personal data which are **manifestly made public by the individual**

f) Processing is necessary for the **establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity

g) Processing is necessary for reasons of **substantial public interest** but must be clearly demonstrated and assessed as part of the public interest test and evidenced throughout the decision making process.

These grounds include the following (the full list of defined purposes may be found in Schedule 1 Part 2 of the Data Protection Act 2018):

- Statutory and government purposes
- Safeguarding of children or individuals at risk
- Legal claims
- Equality of opportunity or treatment
- Counselling
- Occupational pensions

h) Processing is necessary for the purposes of **preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services** on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3

i) Processing is necessary for reasons of **public interest in the area of public health**

j) Processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**

Where there may be difficulty in deciding upon the correct legal basis for processing data, there will be consultation with the Data Protection Officer.

The Trust will comply with Schedule 1 of the Data Protection Act (as well as Articles 6 and Article 9), when processing data where the conditions relate to employment, health and research or substantial public interest as follows:

- Schedule 1, Part 1 of the Data Protection Act 2018 which provides that processing under points (b), (h), (i) or (j) of the GDPR above (conditions relating to employment, health and research).

- Schedule 1, Part 2 of the Data Protection Act 2018 in respect of point (g) above (substantial public interest)

6. Response Times in the Application of Legislation

In applying these regulations Equa MAT is obliged to adhere to the following schedules. The procedures for subject access are detailed in Appendix 1.

a) Subject Access Requests (SARs) whereby an individual may request personal information held by Equa MAT about themselves or a nominated individual on their behalf must be responded to within 1 month,

b) Where the above is found to be complex or numerous an extension may be granted allowing an additional 2 months however the subject must be informed within 1 month of their request,

c) No fee shall be charged for the above except where it is found to be excessive, repetitive or manifestly

unfounded in accordance with the law,

IF APPROPRIATE

d) Freedom of Information Act Requests (FOIAs) whereby an individual may request information held by the council but may not contain information relating to individuals, subject to certain exceptions, must be responded to as soon as possible within 20 working days,

e) No fee shall normally be charged for the above. However in exceptional circumstances a fee may be charged,

f) Environmental Information Regulation requests (EIR) must be responded to as soon as possible but within 20 working days,

g) No fee shall be charged for the above.

7. Rights of the Data Subject

Where consent has been sought as the justification on processing, adequate measures must be in place to record consent and an appropriate method of removing the individual's personal data should consent be revoked must be adopted. In the vast majority of data processing activities a statutory power will be the reason for data processing.

Except where a statutory exemption applies or is in the public interest regarding health an individual who wishes to exercise their right to erasure shall have their personal data removed from all areas where applicable.

An individual when making a SAR is entitled to the following;

a) confirmation that their data is being processed;

b) access to their personal data;

c) other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

8. Data Protection by Design

It is a statutory requirement that any activity involving a high risk to the data protection rights of the individual when processing personal data be assessed by the Data Protection Impact Assessment. Prior to the assumption of any such activity the Data Protection Officer must be consulted and an initial screening be conducted assessing risk.

Any activity involving the processing of personal data must be registered on the Register of processing Activity and reviewed at the very least annually.

9. Data Retention

Except where a specified retention period has been defined in accordance with the purpose of the activity any period of retention is defined by Equa MAT record retention schedule. This is detailed in the Data Retention schedule.

10. Complaints

Where an individual makes a complaint relating to the processing of their personal data or is unhappy with any response to an SAR, FOI or EIR (if appropriate) request they may request an internal review (IR) be conducted. Requests for an IR should be within 40 days of the original response. The responsibility for the conduct of an IR is with Equa MAT who will discuss with the appointed DPO. The school contact is:

The Business Manager Equa
MAT

If an individual is unhappy with the outcome of the IR they have the right to appeal to the Information Commissioner's Office (ICO) for assessment, the ICO is contactable at;

Wycliffe House, Water
Lane, Wilmslow,
Cheshire,
SK9 5AF.

11. Security Incidents

Wherever it is believed that a security incident has occurred or a 'near miss' has occurred, the school and the Data Protection Officer must be informed immediately and the Security Incident Management (SIM) process must be carried out. The SIM is designed to manage, investigate, report and provide 'Learning from Experience' (LFE) to avoid future incidents occurring.

In any case an incident must be reported no later than 24 hours from identification, except where a malicious incident has occurred. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes.

12. Monitoring and Discipline

Compliance with this policy shall be monitored through a review process. This will be agreed with the Data Protection Officer, and compliance will be reported to the senior management board.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the organisation, in consultation with senior management, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

This policy will be reviewed in the light of any change in legislation.

Appendix 1 – Subject Access Request Procedures

The organisation shall complete the following steps when processing a request for personal data (Subject Access Request or SAR) with advice from its Data Protection Officer.

1. Ascertain whether the requester has a right to access the information and capacity.

2. Obtain proof of identity (once this step has been completed the clock can start)

3. Engage with the requester if the request is too broad or needs clarifying

4. Make a judgement on whether the request is complex and therefore can be extended to a 2 month response time

5. Acknowledge the requester providing them with
    a. the response time – 1 month (as standard), an additional 2 months if complex; and
    b. details of any costs – Free for standard requests, or you can charge if the request is manifestly unfounded or excessive, or further copies of the same information is required, the fee must be in line with the administrative cost

6. Use its Record of Processing Activities and/or data map to identify data sources and where they are held

7. Collect the data (the organisation may use its IT support to pull together data sources – for access to emails the organisation can do so as long as it has told staff it will do so in its policies)

8. If (6) identifies third parties who process it, then engage with them to release the data to Equa MAT.

9. Review the identified data for exemptions and redactions in line with the ICO's Code of Practice on Subject Access and in consultation with the organisation's Data Protection Officer.

10. Create the final bundle and check to ensure all redactions have been applied

11. Submit the final bundle to the requester in a secure manner and in the format they have requested.