Data Protection Policy

Prepared by:	Barbara Smith
Date:	20th April 2018
Review date:	April 2019
Approved by:	Board of Trustees 30/4/18

Overview

QEGSMAT is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act 1998 (DPA).

Changes to data protection legislation (GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements.

All staff, governors and Trustees are responsible for data protection.

The Trust Data Protection Officer is **Mrs. Barbara Smith**
Each School in the Trust has a nominated Data Protection Co-ordinator, who is the first point of contact for staff, parents/carers and students in that school.
The Trust is committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them.

The requirements of this policy are mandatory for all staff employed by the Trust and any third party contracted to provide services within the Trust. Non-compliance of this policy and Data Protection Legislation by a member of staff is considered a disciplinary matter, which, depending on the circumstances, could lead to dismissal.

Policy Statements:

The Trust/Academy will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes for which it was collected.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the 'Privacy Notice' and lawfully processed in accordance with the "Conditions for Processing".

Personal and Sensitive Data:

All data within the Academy's control shall be identified as personal, special categories of data or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

Definitions

Personal data: information which relates to an identifiable natural person ('data subject') Examples would be names, dates of birth, addresses, unique pupil number (UPN), exam results, national insurance numbers, appraisal records.

Special categories of data: including information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, biometric data, health, sexual orientation.

Processing data: collecting, using, disclosing, retaining, or disposing of information.

Principles:

The principles of the Data Protection Act shall be applied to all data processed:

- ensure that data is fairly and lawfully processed in a transparent manner
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

Registration:

The Trust is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents / Carers – the 'Privacy Notice':

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all students of the data they collect, process and hold on the students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be available in the new starter pack and on the Trust and academy websites.

Training & awareness:

All staff will receive data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Support and guidance from the Data Protection Officer

Data Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.
Risk and impact assessments shall be conducted in accordance with guidance given by the ICO.
Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and these organisations shall provide evidence of the competence in the security of shared data.

Photographs and Video:

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.

Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources.

Secure Storage of data:

Personal data will be stored in a secure and safe manner. The following measures are taken to help ensure this;
Electronic data will be protected through secure password, encryption software and firewall systems. All users will use strong passwords which must be changed regularly. User passwords must never be shared.

Personal data can only be stored on school equipment (this includes computers and portable storage media. Private equipment (i.e. owned by the users) must not be used for the storage of personal data without the prior agreement of the school's data protection co-ordinator.
As a Data Controller, the Trust is responsible for the security of any data passed to a 'third party'. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party. The Trust will ensure that it is satisfied with controls put in place by third party providers to protect the data.

Paper based personal data will be stored securely where it is not accessible to anyone that does not have a legitimate reason to view or process the data.

Data checking:

Systems will be put in place to ensure the personal data that we hold is up to date and accurate. For example the school will ensure that parents/carers are asked at least once a year to confirm the accuracy of the information we hold.
Any inaccuracies discovered or reported will be rectified as soon as possible.

Disclosing data:

Personal data will not be disclosed to third parties without consent unless it is obliged by law or in the best interest of the child.
Personal data will not be included on the website, in newsletters or other media without consent of the individual (or his/her parents/carers where appropriate). Routine consent will be requested from parent/carers to avoid the need for frequent similar consent being made by the school.
Personal data will only be disclosed to the police if they are able to supply sufficient authority which notifies of a specific, legitimate need to have access to specific personal data.

Data Subject Access Requests:

Any person whose personal data is held by the Trust is entitled under the DPA to ask to access this information. The right is to view or be given a copy of the personal data, rather than to the whole document which contains the personal data.

We shall respond to such requests within one month and they should be made in writing and marked for the attention of the Data Protection Co-ordinator in the relevant school.
No charge will be applied to process the request
Parent/carers can make data subject access requests on their child's behalf if their children are deemed too young to look after their own affairs. If a request is made by a parent for personal data relating to their child and the child is aged 12 years or older, written consent will also need to be sought from the child before the data is disclosed to the parent/carer.

Data Disposal:

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.
For example we will shred or incinerate paper-based records and over write electronic files.
Disposal of IT assets holding data shall be in compliance with ICO guidance: