General Data Protection Regulation (2018)
Policy Statement

Date Published	**June 2016**
Version	**2**
Last Approved Date	**29th April 2020**
Review Cycle	**2 Years**
Review Date	**May 2022**

"Learning together; to be the best we can be"

1. Policy Statement

1.1. The Trust will comply with the Data Protection Act (1998), the General Data Protection Regulation (2018) and Article 8 of the Human Rights Act and will show proper regard for the confidentiality of service users and employees personal information.

1.2. The Data Protection Act came into force on 1st March 2000. It sets rules for those who process personal information to be open about its uses and to follow sound and proper practices when handling personal information. The Act covers all types of records, both manual and electronic. The General Data Protection Regulation (2018) came into force on 25th May 2018 and strengthens the rights of individuals and the use of their data.

2. Definitions

2.1. The following definitions are used throughout this policy statement and in the accompanying guidance notes:

2.2. **Data Protection Act 2018**

Throughout this document, the term Data Protection Act 2018 will be used to encompass the Data Protection Act 1998 and Data Protection Regulation (GDPR) 2018 unless stated otherwise.

2.3. **Data Protection Officer (DPO)**

2.3.1. The responsible person for monitoring internal compliance, informing and advising the accounting office and Directors on data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs) and acting as a contact point for data subjects and the Information Commissioner's Office (ICO).

2.4. **Senior Information Risk Owner (SIRO)**

2.4.1. The person who has overall responsibility for managing records management risks.

2.5. **Data Controller**

2.5.1. The person or organisation who determines how information will be used and for what purpose.

2.6. **Data Processor**

2.6.1. The person who determines the purposes for which and the manner in which any personal data are, or are to be processed.

2.7. **External Data Processor**

2.7.1. A third party who processes information on behalf of the data controller and under their instruction (not an employee). For example, the Trust may use a printing company to print the annual yearbook or employ an agency to serve notices on their behalf. As they will only process information under instruction from the Trust, they will be the data processor and the Trust will remain the data controller for that processing.

2.8. **Data Subject**

2.8.1. The individual about whom you hold the personal information.

2.9. **Information Commissioner's Office**

2.10. The Government Regulator for the Data Protection Act 1998 and Freedom of Information Act 2000 and the named "supervisory authority" as pre the General Data Protection Regulation (2018).

2.11. **Personal Data or Personal Information**

2.11.1. Information which identifies a living individual.

2.12. **Processing**

2.12.1. Obtaining, recording, holding, altering, disclosing, merging, deleting, destroying, retrieving, consulting or using information.

3. The Eight Data Protection Principles

3.1. The following principles apply to all information processed by the Trust and must be complied with.

1. Personal information shall be processed fairly and lawfully and shall not be processed unless certain criteria are met.

2. Personal information shall be obtained for specified and lawful purposes and shall not be further processed in any manner incompatible with those purposes

3. Personal information shall be adequate, relevant and not excessive for the purpose(s) for which they are processed.

4. Personal information shall be accurate and up to date.

5. Personal information shall be kept no longer than necessary for the intended purpose(s).

6. Personal information shall be processed in accordance with the rights of the data subject under this Act (includes an individual's right to obtain copies of their personal information).

7. Appropriate security measures shall be taken against unauthorised or unlawful processing of personal information and against accidental loss, destruction of, or damage to, personal information.

8. Personal information shall not be transferred to a country or territory outside the European Economic Area, unless that country ensures an adequate level of data protection.

4. Individual Rights

4.1. The General Data Protection Act 2018 provides the following rights for individuals:

4.1.1. The right to be informed;
4.1.2. The right of access;
4.1.3. The right to rectification;
4.1.4. The right to erasure;
4.1.5. The right to restrict processing;
4.1.6. The right to data portability;
4.1.7. The right to object;
4.1.8. Rights in relation to automated decision making and profiling.

5. Employee Responsibilities

5.1. Employees who process personal information have an obligation to ensure that the Data Protection Act and General Data Protection Regulation are adhered to and that personal information is not used or disclosed in any way incompatible with the Acts. Information must be handled carefully and employees should not disclose information other than where permitted.

5.2. Employees must also refer to the Code of Conduct regarding standards of confidentiality.

5.3. Employees should take steps to prevent the misuse or unauthorised disclosure of personal information, either intentionally or accidentally, by adopting the following safeguards: -

- Only access information where necessary for work purposes.
- Switch off (or log off) computers when not in use. Only use your own unique user ID to sign onto systems and never disclose these details to anyone else.
- Use all security controls in place such as locking filing cabinets, restricting access to areas, monitoring visitors etc.
- Ensure computer screens cannot be seen by members of the public or employees who have no need to access information.
- Don't disclose information without following established procedures.
- Ensure proper disposal of paper and software containing personal or confidential information.

- Do not remove hardware, software or manual records from Trust premises without prior authorisation. Ensure you follow the guidelines for mobile working within the Information Security Policy.
- If you are unsure about any uses or disclosures of information, take advice from your line manager or Headteacher.

5.4. If an individual is found to have permitted unauthorised disclosure or processing of information, they will be subject to disciplinary action. Individuals and the Trust can face prosecution for breach of the Data Protection Act or misuse of any Trust system or information.

5.5. Employees must also familiarise themselves with the requirements of the Information Security Policy and the Electronic Communications Policy.