Data Protection Policy

Effective Date:	**25th May 2018**
Date Approved/Reviewed:	
Date Due for Review:	**25th May 2020**
Contact Officer:	**School Business Manager**
Approved By:	**Governing Body Resources Committee**

1. Background

The Data Protection Act 2018 replaces the Data Protection Act 1998, and makes provision for the General Data Protection Regulation (GDPR) to be introduced from 25th May 2018. The purpose of the updated legislation is to protect the 'rights and freedoms' of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge.

The school falls within the GDPR definition of a 'data controller' which imposes a duty to comply with a range of conditions regarding how personal data is gathered, stored and managed. The regulation requires the school to nominate a Data Protection Officer to be responsible for ensuring compliance with the GDPR.

This policy will be reviewed on a biannual basis to ensure that it reflects changes to existing legislation, and any new legislation.

2. Policy Statement

In order to operate effectively, the school has to process personal information about people with whom it engages. These may include pupils, parents, current, past and prospective employees and suppliers. In addition, it is required by law to process information in order to comply with the requirements of central government.

The school is committed to ensuring compliance with data protection legislation. It regards the lawful and correct treatment of personal information as essential to its successful operations and to maintaining the confidence of those with whom it carries out business. It fully endorses the principles of data protection by design and default, and will ensure the Data Protection Officer is able to fulfil their tasks as defined in data protection legislation.

Third parties who have access to personal data will be expected to have read and understood this policy. No third party will be able to access personal data without being committed to having obligations no less onerous than the school's. Every effort will be made to ensure data subjects can exercise their rights and any breach of data protection legislation will be dealt with as a matter of urgency. There is a commitment to work with the Information Commissioner's Office (ICO) in all areas relating to

personal data and, if required, breaches will be reported to the appropriate authorities and dealt with as criminal offence.

3. Organisational Requirements

It is the responsibility of the Governors to ensure compliance with Data Protection legislation. However the Head Teacher is responsible for ensuring compliance within the day to day activities of the school.

All those in managerial or supervisory roles are responsible for encouraging good information handling practices. Compliance with data protection legislation and this policy is the responsibility of all employees.

Employees are responsible for ensuring that any personal data about them and supplied by them is accurate and up-to-date. All employees who process personal data are responsible for their own compliance with data protection legislation and this policy. Failure to comply may result in disciplinary action which could lead to dismissal.

Members of the School's Senior Leadership Team (SLT) will jointly fulfil the role of Data Protection Officer (DPO), subject to modifications to their duties to avoid any conflicts of interest. Any division of responsibility between members of SLT will be determined by the Head Teacher. They will be accountable to the Head Teacher and will ensure that the tasks outlined within data protection legislation are fulfilled.

The Head Teacher will periodically present a report to Governors identifying the extent to which the school's responsibilities under the GDPR have been met. The format and content of this report will be periodically reviewed by Governors as necessary.

4. Links with other Policies and Strategies

This policy should be read in conjunction with other relevant policies, for example information technology and human resources.

5. Data Protection Principles

All processing of personal data will be conducted in accordance with the following data protection principles established by the GDPR.

- Personal data will be processed lawfully, fairly and transparently. Some information may only be retained with the specific consent of the individual, although other information used to meet legislative requirements may be retained without consent.
- Personal data will only be collected for specific, explicit and legitimate purposes.
- Personal data will be adequate, relevant and limited to what is necessary for processing.
- Personal data will be accurate and kept up to date with every effort to erase or rectify errors without delay.
- Personal data will be kept in such a form that the data subject can only be identified for as long as is necessary for processing. A retention schedule will be maintained to ensure data is not retained for longer than necessary without the specific approval of the Head Teacher. When data is disposed of, it will be done in a secure manner.
- Personal data will be processed in a manner that ensures a level of security appropriate to the risk and potential impact involved.

- The principles of accountability and good governance will underpin processes implemented to meet the GDPR and will enable the school to demonstrate compliance.

6. Data Subjects' Rights

Every effort will be made to ensure that data subjects are able to exercise the following rights given to them through the GDPR.

- To make subject access requests regarding the nature and purpose of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- To not have significant decisions that will affect them taken solely by automated process.
- To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.
- To request the ICO assess whether any provision of the data protection legislation has been contravened.
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- To object to any automated profiling that is occurring without consent.

Under normal circumstances requests for information will be dealt with within one month and will be processed free of charge, although the deadline may be extended to two months in some circumstances.

In addition, parents have their own independent right under The Education (Pupil Information) (England) Regulations 2006 of access to the official education records of their children. Students do not have a right to prevent their parents from obtaining a copy of their school records. As part of this process the school will apply an appropriate charge for providing copies of records.

Personal data must not be disclosed about a third party except in accordance with data protection legislation. If it appears absolutely necessary to disclose information about a third party, advice should be sought from the DPO.

Data subjects also have the right to complain in relation to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled. This will be done in line with the school's existing complaints policy and procedures.

7. Disclosure of Data

Unless the GDPR gives permission to disclose personal information without consent, personal data will not be disclosed to unauthorised third parties, including family members, friends, suppliers, government bodies and other public sector organisations, unless the request is supported by appropriate documentation. It is the responsibility of employees to ensure that they have the authority to share information and that the recipient is authorised to receive such information. Failure to do so could lead to disciplinary action.

8. Processors and Contracts

The processing of personal data by a third party on behalf of the school will only take place on the basis of a written contract or agreement which clearly specifies both parties' responsibilities and liabilities.

9. Data Inventory

The DPO will maintain an Information Asset Register to record all systems containing personal information covered by the GDPR. This will be used to determine the flows of information through the school, manage risks associated with the processing of particular types of personal data and ensure appropriate systems are put in place to keep information secure.

10. Managing Risk

A risk assessment will be carried out for every information system identified in the Information Asset Register. Where necessary, a more in-depth Data Protection Impact Assessment (DPIA) will be carried out. This is likely to occur where a process is deemed to be high risk or where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, presents a significant risk to the rights and freedoms of an individual. DPIAs will also be carried out in relation to processing undertaken by other organisations on behalf of the school. Where there are significant concerns regarding potential damage or distress, or the quantity of data concerned, the DPO will escalate the matter to the ICO.

To minimise risk in the day to day functioning of the school, guidance will be provided to all staff on a range of issues including:

- Clear Desk and Screen Guidance,
- Handling Personal Data Guidance,
- Privacy Notice and Consent Guidance.

11. Incidents and Breaches

Any data protection incident/breach will be treated as a serious issue and the Head teacher must be informed immediately. The Head teacher will then appoint a member of the Senior Leadership Team to fulfil the role of DPO, taking account of the circumstances of each case to avoid any potential conflicts of interest. Each incident and breach will be investigated by the appointed DPO. An investigation may include Human Resources and Legal Services if there is potential disciplinary action or legal action. In the event that the Head teacher is implicated in any data breach, the School Business Manager will liaise with the council's Data Protection Officer under the terms of the school's Service Level Agreement to ensure the responsibilities of the DPO are effectively discharged.

Certain data protection breaches must be reported by the DPO to the ICO within 72 hours. If required the DPO will also arrange for the affected data subjects to be notified. Any third party processing data on the school's behalf is also required to report data protection breaches to the ICO, and cooperate with the ICO to resolve the issue. They must also notify the school of any breach within the 72 hour window.

The ICO has the authority to sanction significant financial penalties of up to €20 million or 4% of global turnover (fines in the UK will be based on the current exchange rate).

Data subjects' also have a right to compensation if they have suffered material or non-material damage as a result of an infringement of data protection legislation. Any claim for compensation will be dealt with on an individual basis.

12. Training

All staff involved in the processing of data will receive the appropriate training, in order to comply with data protection legislation. Initial training will be followed by regular refresher training. New employees will receive training as part of the staff induction process.

13. References

Data Protection Act 2018
Data Protection Act 1998
https://ico.org.uk/
General Data Protection Regulation - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC
Crime Directive - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644827/LED_Document.pdf
https://www.privacyshield.gov/welcome
Human Rights Act 1998
Freedom of Information Act 2000