G47 DRAFT Data Protection Policy (GDPR)

		Page
1.	Policy Statement	2
2.	Governance and Accountability	2
3.	Definitions	3
4.	Data Protection Principles	3
5.	Legal Basis for Processing	4
6.	Privacy notices	5
7.	Individual Rights	5
8.	Exemptions to the Right of Subject Access	5
9.	Information Society Services to Children	6
10.	Right to Rectification and Erasure	6
11.	Records Management	7
12.	Security	7
13.	Contracts and Data Sharing	8
14.	Data Protection Impact Assessments	8
15.	Data Breaches	9
16.	Compliance Status	9
17.	Policy Revision	9

DATA PROTECTION POLICY

1. Policy Statement

This policy outlines how this School will comply with its responsibilities under the General Data Protection Regulations. Accordingly, it is not intended as a training document, for further details in respect of the GDPR reference should be made to the Information Commissioner's Office "Guide to the General Data Protection Regulation (GDPR)." https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Further it should be noted that at the time of writing the Government has introduced a Data Protection Bill, which is currently progressing through Parliament. Accordingly, this policy will need to be reviewed once that Bill has been finalised.

This policy is supplemental to any other school policies in respect of information management.

The School needs to collect and use certain types of personal information in order for it to provide education and other associated functions. This includes information on current, past and prospective to pupils, parents, staff, contractors, partners and others who come into contact with the School. This personal information must be dealt with properly no matter how it is collected, recorded and used – whether on paper, by computer or recorded on other material.

2. Governance and Accountability

All staff have responsibilities for ensuring the security and safekeeping of the personal information held. Appropriate training will be provided to all staff processing personal data, who are required to complete the training.

Day to day responsibility for ensuring the implementation of this policy will operate under the auspices of the Senior Leadership Team, which in turn will be supported by the Governing Body. Practical guidance in relation to implementation is contained within the ICO guide referenced above.

Overall responsibility for data protection has been delegated to the Assistant Headteacher Mr R.Bruton who is the School's Data Protection Officer and will report to the Governing Body.

A record of internal processing activities will be maintained. Clear, comprehensive and transparent privacy policies and procedures will be maintained.

3. Definitions

'Personal Data' – any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

'Special categories of personal data' – Article 9 of the GDPR refers to sensitive personal data as "special categories of personal data". Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, education outcomes or data concerning a natural person's sex life or sexual orientation.

'Processing' – Obtaining, recording or holding data.

'Data subject' – The person whose personal data is held or processed.

'Data controller' – A person or organisation that determines the purposes for which, and the manner in which, personal data is processed.

'Data processor' – A person, other than an employee of the data controller, who processes the data on behalf of the data controller.

4. Data Protection Principles

The School regards the lawful and proper treatment of personal information as being fundamental to the effective delivery of its objectives and is key to the maintenance of confidence between the School and its pupils, staff and parents.

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of the GDPR requires that personal data shall 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 GDPR in order to safeguard the rights and freedoms of individuals; and
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."

Article 5(2) requires that:

The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

The School will process all personal information to help support the delivery of education in accordance with its aims, responsibilities and obligations. All personal data will be processed in accordance with the principles.

5 Legal basis for Processing

Personal information will only be processed where there is a lawful basis for doing so. Under the GDPR there are six available lawful bases for processing. Which basis is most appropriate to use will depend on the purpose and relationship with the individual.

The lawful bases for processing are set out in Article 6 of the GDPR and in the forthcoming Data Protection Act. The School will ensure that at least one of these will apply whenever the school processes personal data.

In order to lawfully process sensitive data called special personal data in the GDPR, the School must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These do not have to be linked.

Further details in relation to this are at the attached link.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

6. Privacy Notices

The School will, at the point of collection, unless an appropriate exemption applies, inform individuals of the specific purpose or purposes for which the School will use their personal information. To ensure the information required by Article 13 is communicated to the individual.

7. Individual Rights.

The School regards individuals' rights as fundamental and therefore endorses the enhancement of individual data rights as set out in the legislation. All requests for personal information will be dealt with in accordance with the individual's statutory rights. Queries regarding the School's processing of personal data will be dealt with promptly and courteously.

The GDPR provides the following rights for individuals:

1. The right to be informed (Privacy notices).

2. The right of access

3. The right to rectification

4. The right to erase

5. The right to restrict processing

6. The right to data portability

7. The right to object

8. Rights in relation to automated decision-making and profiling.

8. Exemptions – to the Right of Access

The proposed Data Protection Bill introduces exemptions to the Right of access as follows, the right to obtain personal information (subject access) is exempted in

respect of Education Data if its release would be likely to cause serious harm to the physical or mental health of the data subject or another individual.

The right of access does not apply to child abuse data to the extent that the application of the provision would not be in the best interests of the data subject. Child abuse data includes physical injury (other than accidental injury) to, and physical and emotional neglect, ill-treatment and sexual abuse of an individual aged under 18. It consists of data whether they have been subject to or may be at risk of Child abuse.

The right of subject access is exempted in respect of statements of special educational needs where disclosure is prohibited or restricted under the law governing special educational needs and disability. Equally the right is exempted where prohibited or restricted under the Adoption and Children Act 2002 and the Human Fertilisation and Embryology Act 2008.

Further details on individual rights are contained within the attached link:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

9. Information Society Services to Children

The GDPR contains new provisions intended to enhance the protection of children's personal data. Where services are offered directly to a child, the School must ensure that the privacy notice is written in a clear, plain way a child understands. Consent of the child will only be lawful if the Child is at least 13 years of age. Where the child is below this age consent has to be given by the holder of parental responsibility for the child.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/

10. Right to Rectification and Erasure

The GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete. The School will make it easy for individuals to access and correct their personal information. Where a request for rectification is received, the statutory time limit is one month. This can be extended by two months where the request for rectification is complex.

The right to erasure is also known as "the right to be forgotten" and enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. There are some specific

circumstances where the right to erasure does not apply, for example where safeguarding and social services legislation prevents this.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

11. Records Management

Personal information will be held for no longer than is necessary. Appropriate Records Management procedures or policies will comply with this principle.

12. Security

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Appropriate technical and organisational measures will be taken to ensure the security of such data and including:

The pseudonymisation and encryption of personal data;

The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

The regular testing, assessing and evaluating of the effectiveness of technical and organisational measures for ensuring the security of the processing.

Access to personal information will be strictly controlled through the use of password and encryption facilities. Access to systems will be restricted to those users that need it to undertake their duties, access rights will be reviewed on a regular basis. Security measures will be implemented to ensure that personal information is not automatically made widely available.

All staff are made aware of the following requirements.

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal information are kept in a secure location when not in use

- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals. All School laptops have passwords changed regularly.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices if they contain sensitive data.
- Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. For example, we will cross-shred or incinerate paper-based records.

  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

13. Contracts / Data Sharing

When third parties handle data on behalf of the School such as contractors, agents, partners, consultants, etc. there will be a written agreement between the School and the third party confirming that they have appropriate technical and organisational security measures in place to safeguard the personal data and such third parties will only act on the instructions of the School. The School will comply with the further requirements, for third party processing as set out in Article 28 of the GDPR. The School must only appoint contractors who can provide "sufficient guarantees" that the requirements of the GDPR will be met and the rights of individuals are protected.

In sharing personal data the School will follow the Information Commissioner's Guidance in respect of data sharing or the Wales Accord on Sharing of Personal Information.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

14. Data Protection Impact Assessment (DPIA) new systems.

Data protection impact assessments are a tool which can help identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow the School to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

School representatives must carry out a DPIA when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

15. Data Breaches

The GDPR introduces a duty on the School to report certain types of data breach to the Information Commissioner's Office.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data, for example, unauthorised access is also a breach.

If a personal data breach has occurred, the School has 72 hours from the time they become aware of the breach, to report it to the Information Commissioner's Office unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

If the breach is likely to result in a high risk to the rights and freedoms of natural persons we will inform the data subject without undue delay.

16 Compliance Status

Compliance with this policy is mandatory for all staff who have access / use of Personal Information. Breach of this policy by employees may be regarded as gross misconduct and may lead to termination of employment.

17 Policy Revision

This policy has been prepared as at April 2018. At that point, the Data Protection Bill is progressing through Parliament, accordingly this policy should be reviewed when the Bill is finalised. The Information Commissioner's Guidance on the GDPR contains similar provision in relation to review on the finalisation of the Bill.