Data Protection Policy

This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act 1998 and the General Data Protection Regulation 2018.

Please follow this link to the ICO's website (https://ico.org.uk/) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc.

CURRENT

APPROVED – MARCH 2018
REVIEW – MARCH 2021
PERSON RESPONSIBLE – DATA PROTECTION OFFICER

1. Introduction

The Data Protection Act 1998 ("DPA") and the General Data Protection Regulation 2018 ("GDPR") comprise the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the DPA and the GDPR. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

2. Scope of the Policy

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The School needs to keep certain information about employees, pupils and other users to allow it, for example, to monitor performance, achievement, and health and safety. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies. The legal bases for processing data are as follows:-

(a) **Consent**: the member of staff/pupil/parent has given clear consent for the School to process their personal data for a specific purpose.
(b) **Contract**: the processing is necessary for the member of staff's employment contract or other contract.
(c) **Legal obligation**: the processing is necessary for the School to comply with the law (not including contractual obligations).

All staff who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed this Data Protection Policy. This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

3. The Eight Principles

The eight data protection principles or rules for 'good information handling' of the DPA shall apply to all data processed:-

1. Data must be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specific and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.
6. Personal data shall be processed in accordance with the rights of data subjects under the DPA.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. The Data Controller, the Designated Data Controllers and the Data Protection Officer

The School, as a body, is the Data Controller under the DPA, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters. The School has identified its Designated Data Controllers as:

- The Headteacher, Deputy Headteacher, the Business Manager and the Administrative Support Staff.

The Data Protection Officer ("DPO") is the Assistant Head – Inclusion, currently Mr Stan White.

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the DPO in the first instance.

5. Notification

The School's data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

6. Fair Processing and Privacy Notices

The School shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data. Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

There may be circumstances where the School is required either by law or in the best interests of the pupils or staff to pass information onto external authorities, for example local authorities, Ofsted, or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of the School shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them. Under no circumstances will the School disclose information or data:

- that would cause serious harm to a child or anyone else's physical or mental health or condition;
- indicating that a child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child;
- recorded by a pupil in an examination;
- in the form of a reference without consent;
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the School or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed.

7. Disclosure to Third Parties

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

- **Other schools**
  If a pupil transfers from the School to another school, their academic records and other data that relates to their education, health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.
- **Examination authorities**
  This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.
- **Health authorities**
  As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.
- **Police and courts**
  If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.
- **Social workers and support agencies**
  In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.
- **The Department for Education**
  Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.
- External providers of IT, virtual learning and assessment systems eg Parent Pay, PASS, Testbase, 2 Simple, Education City and mymaths

8. Photographs, Videos and CCTV

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

Express prior consent from parents/pupils/staff will be obtained before any use of such images for publication or communication on the website or external media.

It is the School's policy that external parties (including parents) may not capture images of staff or pupils without prior consent.

The School monitors and records CCTV images for the purposes of the health, safety and well-being of the whole school community and the protection of school premises and assets as well as crime prevention. The use of and access to such images is strictly controlled as set out in the School's CCTV Policy in line with the recommendations of the ICO.

9. Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to the School in connection with their employment is accurate and up to date.

- Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.
- Handling all personal data (eg – pupil attainment data) with reference to this policy.

10. Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered as gross misconduct which may lead to dismissal. .

The following guidelines apply:-

- Paper copies of personal data will be kept in a filing cabinet, drawer, or safe in a secure office;
- Computerised personal data will be double-encrypted and password protected and regularly backed up;
- Any computer, laptop, tablet or other mobile device that is being used by staff to process personal data must be double-encrypted, password protected, set up to shut down or sleep after a maximum of 15 minutes and kept secure when not on school premises;
- If information is being viewed on a computer, laptop, tablet or other mobile device, staff must ensure that the window and documents are properly shut down before leaving the device unattended.
- Sensitive information should not be viewed on public computers.
- If personal data is transported from school premises on a USB stick, the data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only.
- Staff must not use their own USB sticks but must use those provided by the School for all and any School-related work. These USB sticks will be double encrypted, password protected and must be kept secure.
- If at all possible, paper copies of data or personal information should not be taken off the school site. If these are misplaced, they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files will be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- Any e mails containing personal data will only be sent using the school Google e mail account which is double-encrypted.
- Wherever possible any data sent by e mail will be anonymised by the use of initials only (without any other identifying data such as date of birth, class or year group).
- Where it is necessary to send documents containing personal data, these will be sent via secure systems such as anycomms secure file transfer or, if that is not possible then before sending by e mail, the document will be password protected and the password sent via a separate e mail to the recipient.

For the avoidance of doubt, members of staff will be able to access their school Google mail account on personal non-encrypted phones for the sole purpose of reading the school bulletin each week. The school bulletin will contain no identifying personal data relating to pupils or families and staff will have given express consent to their initials being used thereon. Those members of staff who choose

not to have their phones encrypted will not use their school Google mail account to send e mails or for any purpose other than to read the bulletin.

11. Rights to Access Information and the Right to be Forgotten

All staff, parents and other users are entitled to:

- Know what information the School holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the School is doing to comply with its obligations under the DPA.

The School will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the DPA to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should make a request in writing and submit it to the DPO. The School will ask to see evidence of identity, such as a passport or driving license, before disclosure of information.

The School will not generally charge on each occasion that access is requested unless the request is manifestly unfounded or excessive (for example, an identical repeat request where very little time has elapsed since the previous request) when a reasonable fee will be charged to recoup any costs of compliance.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the DPA.

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data will be erased by the School including any data held by contracted processors.

12. Retention of Data

The School has a duty to retain some staff and pupil personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time. . In particular, school will only retain copies of safeguarding records where there is an on-going social care involvement and only for a maximum period of either five years after the child has left the school or after any younger sibling has left the school, if relevant.

13. Disposal and Erasure of Data

The School recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk. All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner if they have demonstrable competence in providing secure disposal services. All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process. Disposal of IT assets holding data shall be in compliance with ICO guidance:
https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf

The School has identified a qualified source for disposal of IT assets and collections.