SECURE DATA HANDLING AND DATA PROTECTION POLICY

This policy should be read and understood in conjunction with the following policies and guidance:

- The Data Protection Act (2018)
- The General Data Protection Regulations (2016)
- IRMS Record Management Toolkit for Schools (Toolkit 5 2016)
- Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (DfE September 2018)
- Freedom of Information Toolkit and Procedures
- The school's policies on:
  - Child Protection
  - Online Safety Policy
  - Code of Conduct for Staff

APPENDICES:

Appendix 1	Privacy Notice to pupils
Appendix 2	Privacy Notice to parents
Appendix 3	Privacy Notice to school staff
Appendix 4	Privacy Notice to school governors
Appendix 5	Technical and organisational security measures
Appendix 6	Information Asset Register
Appendix 7	IRMS Record Management Toolkit for Schools
Appendix 8	ICO – Notification of Security Breaches
Appendix 9	Data Subject Access Requests
Appendix 10	Freedom of Information Toolkit and Procedures

CONTENTS:

1. General Principles:

- We recognise that schools have increasing access to a wide range of personal data about pupils, parents and staff, some of which we are legally required to gather and process in order to carry out our duties as a public authority, but also to support the development of pupils (educationally, socially and emotionally), to protect the pupils in our care and to facilitate the efficient running of the school.
- Data and records provide evidence for protecting the legal rights and interests of the school and provide evidence for demonstrating performance and accountability.
- Under the General Data Protection Regulations (GDPR) there are strict legal guidelines in place as to how data should be both 'controlled' and 'processed', which the school is fully aware of and complies with.
- These regulations apply to 'personal data', 'special categories of personal data' and personal data relating to 'criminal convictions and offences'.
- This policy applies to all data and records created, received or maintained by staff of the school in the course of carrying out its functions.

2. Key Definitions:

- **Records** are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created or maintained in hard copy and/or electronically.
- **Personal data** is defined as any information relating to an identifiable person who can be directly or indirectly identified, including by reference to an unique indicator.
- **Special categories of personal data** (previously referred to as 'sensitive data') specifically refers to information held about an individual in the following categories:
  - race
  - ethnic origin
  - politics
  - religion
  - trade union membership
  - genetics
  - biometrics
  - health

  and, as this data, by its very nature could create more significant risks to a person's fundamental rights and freedoms, there are additional safeguards in place.
- **Data controllers** determine the purposes and means of processing personal data.
- **Data processors** are responsible for processing personal data on behalf of a controller.
- **Data protection impact assessments** are required when introducing new technology for the handling and processing of personal data and when data is processed on a large scale. They assess the level of risk involved and the security measures that need to be put in place to protect individuals.
- **Personal data breaches** are defined as a security incident that has affected the confidentiality, integrity or availability of personal data. A personal data breach takes

place whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

- **Subject Access Requests** gives individuals the right to see a copy of the information an organisation holds about them

3. Requirements of the General Data Protection Regulations

- Under the GDPR, the data protection principles (Article 5) set out the main responsibilities for organisations which require that personal data shall be[1]:
  - **a)** processed lawfully, fairly and in a transparent manner in relation to the individual
  - **b)** collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those 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 with every reasonable step being 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 the data subjects for no longer than is necessary for the personal data are processed, and
  - **f)** processed in a manner that ensures appropriate security for the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures

4. Responsibilities:

The school:

- has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment and the person with overall responsibility for this policy is the Head Teacher (for more detail see sections below on '**Documentation**' and '**Accountability and Governance'**
- is required to appoint a Data Protection Officer to oversee the collection, processing and security of data and the person responsible at this school is **XXXXXXXXXXXXXXXXXX** and they can be contacted by **XXXXXXXX**
- as both a controller and processor of personal data, has a responsibility to register with the 'Information Commissioner's Office' and to renew the registration annually
- must inform pupils, parents, staff and governors (through the issuing of **Privacy Notices** – see section below) what data they are required to collect and retain and the lawful basis for processing personal data as defined by Article 6 of the GDPR
- must, through the same Privacy Notices also inform pupils, parents, staff, and governors of any special category data and/or data on criminal convictions or offences, they hold, together with the lawful basis for that processing as defined by Articles 9 and 10 (respectively) of the GDPR

The Data Protection Officer:

- informs and advises the school and its employees about their legal obligations to comply with the GDPR and other data protection laws

[1] See Article 5 of the General Data Protection Act for full legal terminology

- manages internal data protection activities
- advises on data protection impact assessments
- is the first point of contact for external supervisory authorities as well as those individuals (pupils, staff and parents) whose data the school holds

Individual staff and employees:

- must ensure that the records for which they are responsible are accurate and are maintained and disposed of in accordance with the school's records management guidelines. This will form part of staff induction procedures.

Parents/carers, pupils and staff:

- should ensure that the information they provide the school with is accurate and kept up to date

5. Rights of individuals on whom data is held

- The GDPR identified 7 'rights' of individuals on whom data is held, some of which apply to schools and others which are aimed at commercial practices. In this policy we have given guidance regarding each of these rights, but should you wish for more detailed information, this can be found on the ICO website or by clicking on the links below. You can also obtained hard copies of these documents from the school office. They 7 rights as outlined by the GDPR are:
  - right to be informed
  - right of access
  - right to rectification
  - right to erasure
  - right to restrict processing
  - right to data portability
  - right to object
- Some of these rights may not apply, depending on the legal bases on which we hold and process the data.
- Much of the data that schools are required to collect and process falls under our duty as a public authority in order for us to fulfil our legal obligations, and this basis is referred to as our 'public task'. In addition, we also hold data on other bases (as outlined in our Privacy Notices) namely, 'contract' (in relation to the staff we employ) 'consent' 'legitimate interests' and 'vital interests'. The table below shows the rights that apply in 3 areas.

LAWFUL BASIS	RIGHT TO ERASURE	RIGHT TO PORTABILITY	RIGHT TO OBJECT
Public Task	X	X	✓
Contract	✓	✓	X
Consent	✓	✓	X
Legitimate Interests	✓	X	✓
Vital interests	✓	X	X

- **Right to be informed**: **(Please also refer to the section below on 'Privacy Notices')**
  At the time of requesting data from individuals (pupils, parents, staff, governors), the individuals must be informed of their rights regarding that data, which should include:
  - the name and contact details of the school's Data Protection Officer

  - the categories of personal data
  - the school's purpose and lawful process/es for processing data the categories of personal data being requested
  - the legitimate interests that apply where that is the lawful basis
  - who the data is shared with
  - how long it is held for
  - the right to withdraw consent at any time (where relevant depending on the lawful basis)
  - the right to lodge a complaint with a supervisory authority (the ICO)
  - whether the provision of personal data is part of a statutory requirement and the possible consequences of failing to provide the personal data, and
  - the existence of any automated decision making, including profiling and information about how decision are made, the significance and the consequences
- In addition, there may be times during the school year when we may require further information from you for a specific purpose. At that time, will advise you of any additional information regarding your rights as we are required to do by the GDPR.
- If we are reliant on 'consent' as our lawful basis, you will be advised of that and you will be required to give your consent in writing.
- **Right of access:** All individuals have the right to access their personal data and supplementary information and this is referred to as a 'Subject Access Requests (SAR)'. Appendix 9 gives more information on SAR in the form of 'Frequently Asked Questions'.
  - The right of access allows individuals to be aware of and verify the lawfulness of the processing of their data.
  - Individuals have the right to be provided with a copy of the information that is held on them free of any charge unless the request is manifestly unfounded, excessive or repetitive, in which case the school reserves the right to charge a reasonable fee, based on the administrative costs of providing that information.
  - A reasonable fee may also be charged for further copies of the same information.
  - Information must be provided without delay and at the latest within one month of receipt of the request, or longer depending on when the request is made (see final bullet point).
  - Where the requests are complex or numerous, the school can extend the compliance period for a further two months as long as the individual requesting the information is informed that this will be the case within one month of the receipt of the request. The school will, at the same time, explain why this extension in time is necessary.
  - Whilst it is always our aim to respond in a timely manner, given the nature of the school's academic year, should a request be received less than one month before the end of any term or within a school holiday period, the school will require an extended period of time in which to comply and this will be explained to the applicant at that time.
  - The school reserves the right to refuse to respond to a request when they are manifestly unfounded or excessive, especially in they are repetitive. In such cases, the individual making the request will be informed of the school's decision not to comply together with the reason why, as well as informing them of their right to complain to the supervisory authority without delay and at the latest within one month.

  - Where the request is made electronically, the school will provide the information requested in a commonly used electronic format.
- Where we hold a large amount of personal data about an individual, we can ask that the request be specific.
- **Right to rectification:**
  - Individuals have the right to have their personal data corrected if it is inaccurate or incomplete.
  - Where the school has disclosed this information to a third party (e.g. Department for Education or Local Authority) it is responsible for ensuring that the third party also corrects the data in question. The individual will be advised of any third parties to whom the data has been supplied, where appropriate.
  - The school must ensure that data is rectified within one month but we may extend this period for a further two months where the request is complex.
  - Where the school decides not to take action to rectify data at the request of an individual, we will explain why and inform them of their right to complain and to whom that complaint should be addressed.
- **Right to erasure**: Individuals have the right to request that their information is erased/deleted where there is no compelling reason for its continued processing i.e.:
  - where it is no longer necessary for the school to hold that data (bearing in mind the requirement to retain certain documents for a specific period of time[2])
  - when, if the data is obtained under the basis of 'consent' that consent is subsequently withdrawn
  - where data has been unlawfully processed or where an individual objects to the processing and there is no overriding legitimate interest for the processing to continue.
- **Right to restrict processing:** In certain circumstances, individuals have the right to request the restriction or suppression of their personal data, which means that they can limit the way in which any organisation uses their data.
  - This right applies when:
    - an individual contests the accuracy of the data being processed
    - an individual believes that data has been unlawfully processed
    - the school no longer needs to keep the data but has been asked to do so in order to establish, exercise or defend a legal claim
    - an individual objects to the processing of the data and the school is considering whether its legitimate grounds override those of the individual in question.
  - The school can refuse to comply with a request for restriction if we believe the request to be manifestly unfounded or excessive (taking into account whether it is repetitive in nature) and we may either refuse to deal with the request or reserve the right to charge a fee in order to deal with it.
  - We will justify our decision for any action we take in writing. In the event that we do refuse to comply or wish to charge a fee, individuals will be informed within one month of the receipt of the request (with exceptions being made for school holidays) and will advise individuals of our reasons, their rights to make a complaint to the ICO and their rights to seek a judicial remedy.

[2] IRMS – Toolkit 6 for schools (Appendix 7)

- Should the school decide it is appropriate to charge a fee or believe that we require additional information to identify an individual, no further action will be taken before that fee is received, after which the school still has one month to respond.

- **Right to data portability**: The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller.
  - The right to data portability only applies when:
    - the lawful basis for processing this information is consent **or** for the performance of a contract; and
    - the school is carrying out the processing by automated means (ie excluding paper files)
- **Right to object**: Where applicable, individuals have the right to object on "grounds relating to their particular situation".
  - Where an individual exercises their right to object, we are required to stop processing the personal data we hold unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims.
  - Individuals are advised on their right to object in our Privacy Notice

6. <u>Privacy Notices:</u>

- The school, in compliance with the requirements of the GDPR, will issue Privacy Notices to all individuals on whom we hold data, at the time that they join our school, namely:
  - pupils (via their parents),
  - parents
  - staff
  - governors
- (See Appendices 1, 2,3 and 4 Copies of our Privacy Notices to pupils and parents can also be found on the school website.
- Our Privacy notices will contain the following information:
  - the categories of data that we hold
  - why we collect it
  - the lawful basis on which we process that data
  - who we share the data with
  - how long we retain the data
  - your right to access your data and your right to object

7. <u>Documentation</u>

- The GDPR contains explicit provisions regarding what we are required to document regarding the data we control. Article 30 states that we must document the following information (available both in electronic form on our website and as a paper copy, which can be obtained by request from the school office :
  - the name and contact details of our organisation
  - the contact details for our data protection officer
  - the purpose of our processing
  - descriptions of the categories of individuals and categories of personal data
  - who receives the personal data we process
  - our retention schedules (which are based on the IRMS Toolkit – Appendix 7)
  - a description of our technical and organisational security measures (see Appendix 5)

- To this end, we have produced and maintained an 'Information Asset Register' (Appendix 6) in which we record the following information:
  - descriptions of the data that we hold (personal data, special category data and data relating to criminal convictions and offences)
  - the lawful basis for our processing with reference to Articles 6, 9 and 10 of the GDPR
  - in what format and how that data is held
  - how long we retain the data for

8. Accountability and Governance

Under the GDPR, the school is required to demonstrate that we comply with the principles of the accountability and responsibility and in order to do this we must:

- ensure that we implement appropriate technical and organisation measures which will include:
  - publication of this policy
  - on-going training for staff and induction for new staff
  - internal audits of our processing activities, including data protection impact assessments for personal and/or special category data that is processed on a large scale
  - internal audits of all the personal data we hold, including special categories of personal data which include the form that the data is held in, where it is held, who has access to it, the security measures in place and how long it is retained for
- ensure that our records are kept up to date and reflect our current position, and
- in the unlikely event of a data breach, (see 8 below on Personal data breaches) we will ensure that records are kept regarding the breach and the action we took in response to it.

9. Personal data breaches

- Personal data breaches can include:
  - access to the data we hold by an unauthorised 3rd party
  - deliberate or accidental action (or inaction) by a controller or processor
  - sending personal data to an incorrect recipient
  - computing devices containing personal data being lost or stolen
  - alteration of personal data without permission; and
  - loss of availability of personal data.
- The school needs to ensure that there are robust systems in place to detect, investigate and report any breaches of personal data.
- The GDPR makes it clear that when a security incident takes place, we are required, as a matter of urgency, to establish whether a personal data breach has occurred and, if so, promptly take steps to address it. Some data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job whilst other breaches can significantly affect individuals who personal data has been compromised. This needs to be assessed this on a case by case basis.
- Under the GDPR we are required to report a personal data breach within 72 hours, when it is felt that as a result of that breach there is likelihood of a risk to people's rights and freedoms. A breach can have a range of adverse effects on individuals which might include emotional distress and/or physical and material damage. Where it is not felt that this risk is likely, it is not necessary to report the breach but we will still document

the breach and justify the decisions that have been taken, together with any subsequent action.

- Where the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms we will inform those individuals without undue delay.
- When reporting a breach, we are required to provide the GDPR with the following information:
  - a description of the nature of the personal data and, where possible, the categories and number of individuals concerned together with the category and number of personal date records concerned
  - the name and contact details of our Data Protection Officer
  - a description of the likely consequences of the personal data breach; and
  - a description of the measures taken, or proposed to be taken, to deal with the personal data breach including, where appropriate, the measures taken to mitigate any possible adverse effects.
- See Appendix 8 for more detailed information on the process of reporting data breaches as well as from the ICO's website.[3]
- We will keep records of any data breach, whether or not we are required to inform the ICO

10. Freedom of Information

The school understands its obligations under the Freedom of Information Act 2000 and the procedures and supporting documents which explain the process can be found in Appendix 10

11. Policy review

- This policy will be reviewed every ….. years or earlier in the event of any changes to legislation.

[3] ICO's guidance to reporting a data breach