1. Legal Framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

1.2. This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- All Article 29 Working Party Guidance on the implementation of GDPR
- Department of Education 'Data Protection: a toolkit for schools'
- IRMS Information Management Toolkit for Schools.

2. Applicable Data

For the purpose of this policy:

2.1 Personal data refers to information that relates to an identified or identifiable, living individual (Data Subject), including an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.2 Sensitive personal data is defined in the GDPR as 'special categories of personal data', which includes the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

2.3 Processing Data is referred to throughout the GDPR and data protection legislation. This means any use of the personal information which includes collecting, disclosing, destroying, archiving and organising.

2.4 Data Subject is the person who the personal data is about. For example, the children named on a class register at a school are all data subjects of that register.

2.5 Data Controller is usually an organisation who dictates the reason and purpose for how data is processed. The Council itself is a Data Controller as it chooses how it collects, uses and shares its own data. The Trust has appointed a nominated Data Protection Officer and a Trust School's Data Protection Lead.

2.6 The Information Commissioner's Office (ICO) is the regulator for Data Protection and Privacy law in the UK. They have the power of enforcement with organisations for breaches of the Data Protection Act or the GDPR. This means they can issue: -

- An Undertaking which commits an organisation to improving their Data Protection practices.
- An Enforcement Notice ordering that an organisation does something specific e.g. train all staff to a high standard.
- A Monetary Penalty for serious and significant breaches. Under the Data Protection Act, this can be a penalty up to £500,000. Under the General Data Protection Regulation this can be up to €20 Million or 4% of a company's (MAT's) turnover.

2.7 This policy applies to both automated personal data and to manual filing systems.

3. Principles

3.1 In accordance with the requirements outlined in the GDPR, personal data will be:

1. Processed Fairly, Lawfully and Transparently
2. Processed for a Specified and Legitimate Purpose
3. Adequate, Relevant and limited to what is relevant
4. Accurate and up to date
5. Kept no longer than necessary
6. Stored securely using appropriate technical and organisational measures.

3.2 The GDPR also requires that "the controller (the Trust)) shall be responsible for, and able to demonstrate, compliance with the principles".

4. Accountability

4.1 The Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in the line with the principles set out in the GDPR. This can take a variety of forms. Examples of technical and organisational measures can be found below.

Technical Measures

- Firewalls
- Anti-virus software
- Encryption
- Secure emails

Organisational Measures

- Policies and Procedures in place to help staff understand their duties to maintain data protection
- Training
- A more knowledgeable and open culture towards embedding Data Protection

4.2 The Trust will provide comprehensive, clear and transparent privacy notices.

4.3 Records of activities relating to higher risk processing will be maintained, such as the processing of special categories of data.

4.4 In line with best practice, the Trust shall maintain a record of processing activities will include as a minimum the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures

4.5 The Trust will meet the principles of data protection, continuously creating and improving security features.

4.6 The Trust will produce Data Protection Impact Assessments where the processing of personal data is likely to result in a high risk to the rights of the individual, where a major project requires the processing of personal data or before the introduction of new technology or a significant change to the way processing is performed.

5. Data Protection Officer (DPO)

5.1 The Trust will has appointed a nominated DPO in order to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

5.2 The Trust will make freely available the contact details for their appointed DPO:

Trust's Data Protection Officer
gdpr@imperosoftware.com
(0330) 400 4142

5.3 The DPO will operate independently, their role being to:

- advise the Trust, each school and its employees about the obligations to comply with GDPR and other data protection requirements – this could be to assist in implementing a new CCTV system or to respond to questions or complaints about information rights.
- monitor the Trust's and each school's compliance with GDPR, advising on internal data protection activities such as training for staff, the need for data protection impact assessments and conducting internal audits.
- act as the first point of contact with the Information Commissioner's Office and for individuals whose data we process.

5.4 Where advice and guidance offered by the DPO is rejected by the Trust or any school, this will be independently recorded and the Trustees advised.

5.5 Advice offered by the DPO will only be declined at the direction of the Head and/or LEC and will be provided to the DPO in writing.

6. Lawful Processing

6.1 The legal basis for processing data will be identified and documented prior to data being processed. The trust will make it clear, at all times, the basis on which personal data is processed.

6.2 The Trust will ensure that, where it processes personal data it will be lawfully processed under one of the following conditions:

- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For the performance of a contract with the data subject or to take steps to enter into a contract.
- Protecting the vital interests of a data subject or another person.
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

6.3 In addition, the school will ensure that the processing of sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Protecting the vital interests of a data subject or another individual here the data subject is physically or legally incapable of giving consent.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for the establishment, exercise or defence of legal claims
- Processing is necessary for reasons of substantial public interest, on the basis of Union or Member state law, with full regard for the rights and interests of the data subject.
- Processing is necessary for the purposes of preventive or occupational medicine, for example, t the assessment of the working capacity of the employee
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

7. Consent

7.1 Where there is no other legal basis for the processing of data the Trust may rely on the consent of individuals, both parents and pupils, in seeking consent.

7.2 Where used, consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

7.3 Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

7.4 Where consent is given, a record will be kept documenting how and when consent was given.

7.5 Consent previously accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

7.6 Consent can be withdrawn by the individual at any time.

7.7 The consent of parents will be sought prior to the processing of a child's data under the age of 12 except where the processing is related to preventative or counselling services offered directly to a child.

8. The Right to be Informed

8.1 The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

8.2 If services are offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

8.3 In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, and where applicable, the controller's representative and the DPO.
- The purpose of, and the legal basis for, processing the data.
- Any legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
- Withdraw consent at any time.
- Lodge a complaint with a supervisory authority.

8.4 Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

9. The Right of Access

9.1 Individuals have the right to obtain confirmation that their data is being processed.

9.2 Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. A form for requesting information is available from the school

9.3 The Trust will verify the identity of the person making the request before any information is supplied as well as confirming the subject of the request and the right to make such a request (see 9.12. and 9.13)

9.4 A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

9.5 Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

9.6 Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee may be charged.

9.7 All fees will be based on the administrative cost of providing the information.

9.8 All requests will be responded to without delay and at the latest, within one month of receipt.

9.9 In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

9.10 Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

9.11 In the event that a large quantity of information is being processed about an individual, the school may ask the individual to specify the information the request is in relation to.

9.12 A parent or guardian does not have an automatic right to information held about their child. The right belongs to the child and the parent(s) acts on their behalf, where they have parental responsibility for the child. In England the age at which a child reaches sufficient maturity to exercise their own right to access their information is normally 12, but this may vary amongst individuals. Once a child reaches sufficient maturity, the parent may only act with their child's consent.

9.13 Where a child is over 12 and a request is made on their behalf, the Trust may contact them separately to seek their signed consent for someone to access their records on their behalf. When deciding whether information about a child can be released, consideration will be given to the best interests of the child.

9.14 The Trust will clearly communicate and promote the process for the submission of Subject Access Requests and the exercising of other individual rights as defined under the GDPR during holiday periods, stating clearly how the Trust will handle these requests and how this may impact on any time scales.

10. The Right to Rectification

10.1 Individuals are entitled to have any inaccurate or incomplete personal data rectified.

10.2 Where appropriate, the Trust will inform the individual about the third parties that the data has been disclosed to.

10.3 Where the personal data in question has been disclosed to third parties, the Trust will inform them of the rectification where possible.

10.4 Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

10.5 Where no action is being taken in response to a request for rectification, the trust will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

11. The Right to Erasure

11.1 Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

11.2 The right to erasure is not absolute. Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent

- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation

11.3 The Trust has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

11.4 As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

11.5 Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

11.6 Where personal data has been made public within an online environment, the Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question where possible.

12. The Right to Restrict Processing

12.1 Individuals have the right to block or suppress the Trust's processing of personal data.

12.2 In the event that processing is restricted, the Trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

12.3 The Trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the Trust has verified the accuracy of the data
- Where an individual has objected to the processing and the Trust is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the Trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

12.4 If the personal data in question has been disclosed to third parties, the Trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

12.5 The Trust will inform individuals when a restriction on processing has been lifted.

13. The Right to Data Portability

13.1 Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

13.2 Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

13.3 The right to data portability only applies in the following cases:

- To personal data that an individual has provided to the Trust
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

13.4 Personal data will be provided in a structured, commonly used and machine-readable form.

13.5 The Trust will provide the information free of charge.

13.6 Where feasible, data will be transmitted directly to another organisation at the request of the individual.

13.7 The Trust is not obligated to adopt or maintain processing systems which are technically compatible with other organisations.

13.8 In the event that the personal data concerns more than one individual, the Trust will consider whether providing the information would prejudice the rights of any other individual.

13.9 The Trust will respond to any requests for portability within one month.

13.10 Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

13.11 Where no action is being taken in response to a request, the Trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14. The Right to Object

14.1 The Trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

14.2 Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing undertaken by or on behalf of the Trust
- Processing for purposes of scientific or historical research and statistics.

14.3 Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

14.4 Where personal data is processed for direct marketing purposes:

- The Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

14.5 Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Trust is not required to comply with an objection to the processing of the data.

14.6 Where the processing activity is outlined above, but is carried out online, the Trust will offer a method for individuals to object online.

15. Privacy by Design and Data Protection Impact Assessments

15.1 The Trust will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities.

15.2 Data Protection Impact Assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

15.3 DPIAs will allow the Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Trust's reputation which might otherwise occur.

15.4 A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

15.5 A DPIA may be used for more than one project, where necessary and where the aims and conditions of the project are the same.

15.6 The Trust will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

15.7 Where a DPIA indicates high risk data processing, the Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

16. Data Processors

16.1 The Trust will ensure that whenever it employs or utilises a data processor a written contract will be in place.

16.2 Any contract will include, as a minimum, specific terms under which processing is allowed and will document:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;

- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

16.3 Where appropriate, and if and when supplied by the Information Commissioner's Office, standard clauses may be supplemented.

16.4 Any contract will clearly identify the responsibilities and liabilities of data processors in relation to:

- not to use a sub-processor without the prior written authorisation of the data controller;
- to co-operate with supervisory authorities (such as the ICO);
- to ensure the security of its processing;
- to keep records of processing activities;
- to notify any personal data breaches to the data controller;
- to employ a data protection officer; and
- to appoint (in writing) a representative within the European Union if needed.

16.5 Where a processor fails in these obligations or acts outside of the direct instructions of the school, appropriate remedial action will be taken promptly.

17. Data Breaches

17.1 The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

17.2 The Trust will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their continuous development training.

17.3 Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

17.4 All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it by the school's Data Protection Officer.

17.5 The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

17.6 In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Trust will notify those concerned directly.

17.7 A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

17.8 In the event that a breach is sufficiently serious, the public will be notified without undue delay.

17.9 Effective and robust breach detection, investigation and internal reporting procedures are in place at the Trust, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

17.10 Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

17.11 Failure to report a breach when required to do so will be a breach of school policy and an additional breach of the GDPR.

18. Data Security

18.1 Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

18.2 Confidential paper records will not be left unattended or in clear view anywhere with general access.

18.3 Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

18.4 Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

18.5 All electronic devices are encrypted and password-protected to protect the information on the device in case of theft. Staff must not leave their access password with their laptops.

18.6 Staff will not use their personal laptops or computers for Trust purposes.

18.7 All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

18.8 Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient. Governors, Trustees and Members will not use personal emails to send or receive sensitive information.

18.9 Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

18.10 Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the Trust's premises accepts full responsibility for the security of the data.

18.11 Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

18.12 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

18.13 The physical security of the Trust's buildings and storage systems, and access to them, is reviewed on an annual basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

18.14 Any unauthorised disclosure or personal or sensitive information may result in disciplinary action.

19. Publication of Information

19.1 The Trust will not publish any personal information, including photos, on its website, in social media or in any promotional or marketing publication without the permission of the affected individual.

19.2 When uploading information to the Trust's or individual school's website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

20. CCTV

20.1 The Trust operates CCTV on all premises and is mindful of the GDPR implications of this. A separate CCTV policy is held by the Trust and is available for inspection on the Trust's website.

20.2 Requests for access to CCTV are covered in both the CCTV policy, for general requests, and the information Rights Policy, for Subject Access Requests.

21. Data Retention

21.1 Data will not be kept for longer than is necessary in line with the schools Record Management Policy.

21.2 Unrequired data will be deleted as soon as practicable.

21.3 Paper documents will be shredded, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

22. DBS Data

22.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

22.2 Data provided by the DBS will never be duplicated.

22.3 Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.