Data Protection Policy

Review Period	Two Yearly
Person Responsible for Policy	Chief Executive
Governing Committee	Trust Board
Date of Trustees Approval	February 2019
Date for Review	February 2021

1. Introduction

1.1. This Data Protection Policy ("Policy") regulates and details the way in which ("the Trust") and "the School" (Schools within the Trust) obtain, use, hold, transfer and process Personal Data and Sensitive Personal Data (as defined in parts 2 and 7 of this policy) about individuals and ensures that all Trust employees know the rules for protecting Personal Data.

1.2. This Policy also describes individuals' rights in relation to the Personal Data processed by the Trust.

1.3. The Trust has practices in place in relation to its handling of Personal Data to ensure that they are acting in accordance with UK laws and other relevant regulatory guidance. The most notable legislation in this area is the Data Protection Act 1998 (DPA) and the General Data Protection Regulation (GDPR) enacted in 2018.

1.4. The Trust shall comply with the principles of the DPA to ensure that all data is:

- Fairly and lawfully processed
- Processed only for lawful purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without consent and adequate protection

In addition, the Trust will also comply with the GDPR that introduces further rights for individuals and strengthens some of the rights already in existence under the DPA:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

At all times, the Trust will endeavour to ensure that it has a legal basis for the processing of personal information.

1.5. ("the Trust") is registered as a Data Controller with the Information Commissioner's Office (ICO). The Trust's Data Protection Officer is available to contact on any Data Protection issue.

2. Personal Data

2.1. "Personal Data" is any information (for example, a person's name) or combination of information about a living person (such as name and address and date of birth) which allows that living person to be identified from that information and which relates to them, such as the job application of "Joe Green" with his address and date of birth, or the academic record

of "Sam Brown" with similar details. If in doubt, individual details should be treated as Personal Data.

2.2. Examples of Personal Data which may be used by the Trust in its day to day business include employee, pupil, parent and customer details, such as names, addresses, telephone numbers and other contact details, such as email addresses and mobile numbers, CVs, performance reviews, photos, payroll and salary information. This could affect job applicants, direct employees, temporary staff, volunteers, parents, pupils, individual consultants or contractors, visitors etc.

2.3. Personal Data may also be relevant to unincorporated suppliers or customers (such as a sole trader business or partnership), or inquirers or complainants, and to individual contacts at third parties, customers and leads, even in respect of work contact details, such as their direct line or mobile number, or information entered about them in any management system.

2.4. The definition of Personal Data also includes opinions about a person, and appraisals about or statements of intent regarding them.

2.5. The laws governing how the Trust can use Personal Data apply whether the Personal Data is stored electronically (for example, in emails, on IT systems, as part of a database or in a word processed document) or in structured paper records (for example, in paper files, card indexes or filing cabinets).

3. Processing of Personal Data & Audits

3.1. The Trust uses or processes Personal Data (including Sensitive Personal Data, see section 7) on a range of individuals for a multitude of business purposes, including the use of CCTV systems. Such individuals may include staff and contractors, pupils and parents, alumni, business contacts, customers and prospects, job applicants and former employees, and the person whose Personal Data is used by the Trust is known as "the data subject".

3.2. When the Trust collects, stores, uses, discloses, updates or deletes or destroys Personal Data, this is called "processing". All processing is regulated by data protection legislation and must meet certain conditions to be carried out lawfully.

3.3. The Trust maintains a database of personal data held in different Trust departments, has clear retention schedules and the Data Protection Officer conducts regular audits of Personal Data held.

3.4. Personal Data and Sensitive Personal Data are held securely by the Trust and staff are regularly briefed on appropriate and safe data management.

4. Legislation and Information Commissioner's Office

4.1. Data protection laws are enforced in most countries by the local Data Protection Authority, in the UK being the Information Commissioner's Office ("the "ICO"). The ICO may investigate concerns and complaints, may audit the Trust's use or processing of Personal Data and may take action against the Trust (and in some cases individuals) for breach of these laws. Action may include making the Trust pay a fine and/or stopping the use by the Trust of the Personal Data, which may prevent it from carrying on its business. There is also the risk of negative publicity.

4.2. In addition, the General Data Protection Regulation (GDPR) will replace the current EU Directive in May 2018 and will be directly applicable in all Member States (and those wishing to engage and trade with those states) without the need for implementing national legislation. This introduces more stringent data protection obligations on Data Controllers.

5. Transparency and Personal Data

5.1. The Trust is entrusted to use the Personal Data of individuals on the basis that the proposed use is transparent, expected and clearly defined. Accordingly, one of the main data protection obligations requires the Trust to process Personal Data fairly.

5.2. In addition, use of Personal Data must be lawful. In practice, this means that the Trust will comply with at least one of the following conditions when processing Personal Data:

a) the individual to whom the Personal Data relates has consented to the processing;
b) the processing is necessary for the performance of a contract between the Trust and the individual (or to enter into that contract at the individual's request);
c) the processing is necessary to comply with a legal obligation (not a contractual obligation) placed on the Trust;
d) the processing is necessary to protect a vital interest of the individual (where there is an imminent risk to their life or of serious harm to them otherwise); or
e) the processing is necessary to pursue the legitimate interest of the Trust (or a proposed recipient of the Personal Data) but where on balance, this would not involve disproportionate harm to the individual.

5.3. Use of Personal Data should meet one or more of these conditions. If there are any concerns about this; it is proposed to use Personal Data for additional purposes; or new reasons for using Personal Data are contemplated, reliance on these conditions must be discussed in the first instance with the Data Protection Officer prior to being relied upon.

5.4. All new Personal Data processing activities and projects involving the use of Personal Data must be approved prior to being started as there are complex exemptions and other lawful reasons for processing which may apply. For example, if someone provides their details as a contact, you will not be able to start sending them marketing emails unless that is covered in an appropriate notice and consent from that individual.

5.5. In addition, the Trust ensures its Personal Data is accurate and up to date. The Trust takes care to record and input Personal Data accurately. Some Personal Data may change from time to time (such as addresses and contact details, bank accounts and the place of employment). It is important to keep current records up to date. The Trust takes care to update records promptly and correctly.

6. Privacy Notices

6.1. When an individual gives the Trust any Personal Data about him or herself, the Trust will make sure the individual knows:

a) who is responsible for the Processing of their Personal Data;
b) for what purposes that Trust will process the Personal Data provided to it;
c) sufficient details about any proposed disclosures/transfers of their Personal Data to Third

Parties (including any cross border transfers);
d) the rights that the individual has in respect of their personal data;
e) any other information that the individual should receive to ensure the processing carried out is within his/her reasonable expectations (retention periods for instance); and f) who to contact to discuss or raise any Personal Data issue.

6.2. The Trust does this by providing this information in a "privacy notice" or fair processing notice. Before collecting Personal Data, staff at the Trust will give individuals providing those details appropriate Privacy Notices, these may be embedded in contracts, or on websites or form part of application or other forms. The Trust will inform individuals about the processing of their Personal Data before or at the time the data is collected. The information contained in its Privacy Notices will be concise and easily accessible and written in clear and plain language.

6.3. The Trust will only process Personal Data in a manner and for purposes consistent with the relevant privacy notice(s) already provided to an individual. Personal Data should not be collected for one purpose and then used for a second purpose unless that is also set out in the relevant notice.

7. Sensitive Personal Data

7.1. "Sensitive Personal Data" is Personal Data about a person's race or ethnicity, their health, their sexual preference, the medical information,their religious beliefs, their political views, trade union membership or information accusing an individual of any crime, or about any criminal prosecution against them, and the decision of the court and any punishment. The Data Protection Officer can provide further information on what is, and the handling of, Sensitive Personal Data.

7.2. Sensitive Personal Data should not be collected or used unless essential. It must be treated as strictly confidential. Extra care must be taken with it and it must be kept more securely. In addition to the normal requirements for lawful use of any Personal Data such details should not be used without the explicit prior consent of the individual, which has to be clear, unambiguous and voluntary.

7.3. The Trust does not seek to obtain Sensitive Personal Data unless:

a) the individual concerned agrees in writing that we may do so, on the basis of a full understanding of why the Trust is collecting the data
b) the Trust needs to do so to meet its obligations or exercise its rights under any relevant laws; or
c) in exceptional circumstances such as where the processing is necessary to protect the vital interests of the individual concerned

Please note that the "legitimate interest" criteria described above (in section 5.2e) alone is not enough to process Sensitive Personal Data.

7.3. Sensitive Personal Data should not be disclosed unless measures are taken to encrypt or otherwise secure that information due to the potential for harm or distress if the email is received by unintended recipients or otherwise goes astray.

7.4. Sensitive Personal Data should be collected and used as little as possible and be subject to more limited and strictly need to know access, and used subject to greater security measures than other Personal Data.

7.5. Other Personal Data where misuse may lead to distress or harm, especially to fraud or identity theft (for example, bank account or credit card details, or official government identification numbers, such as national insurance contribution numbers) must be treated like Sensitive Personal Data.

8. Employee Obligations

8.1. All Trust staff should be aware of their obligations and comply at all times with this Policy.

8.2. All staff must ensure that Personal Data collected by them must be appropriate to and sufficient for the relevant purpose(s) for which it is collected but not excessive for that purpose(s). Use of Personal Data should be minimized and not maximized. Collecting unnecessary personal Data adds to the Trust's compliance burden. Where staff are dealing with pupil and parent data already collected by the Trust (on iSams for example), the individual/s concerned will have given consent on joining the Trust for the processing of their personal data for the purposes of running the Trust.

8.3. All staff involved in the processing of personal information will:

- Read and understand this policy
- Use strong passwords
- Encrypt all portable devices if they contain personal data
- Only keep information as long as necessary
- Staff should not download personal data onto personally owned devices unless absolutely necessary. In such cases, the personal data should be deleted from the personal device as soon as is practicable after use.

9. Data retention & Trust Archives

9.1. Personal Data must be stored securely and not be kept for any longer than required. Some records have to be retained for minimum periods by law (such as records on employee payments and their taxation under tax laws).

9.2. As a general rule, when Personal Data is no longer needed for the purposes for which it was collected, this Personal Data will be securely and permanently destroyed as soon as practicable.

9.3. The Trust will not delete or destroy or amend records containing Personal Data without explicit consent once they have been informed those records have been requested by the individual whose Personal Data it is, or by a Data Protection Authority. Such a breach may be a criminal offence with personal liability.

10. The Right to Information, the Right to Erasure and Subject Access Requests (SAR)

10.1. Individuals have certain rights in relation to their Personal Data:

a) the right to obtain information (what Personal Data, from where, used for what purposes and shared with which recipients) about Personal Data held about themselves and to obtain copies of such Personal Data (Subject Access Request);
b) the right to prevent processing of Personal Data for direct marketing purposes;
c) the right to object to and stop certain processing of Personal Data where it is likely to cause substantial unwarranted harm or distress;
d) the right to have Personal Data corrected;
e) the right to compensation for any damage/distress suffered from any breach;

f) the right to be informed of automated decision making about them.

10.2. If any member of Trust staff receives such a request or demand from an individual, they must promptly inform the Data Protection Officer.

10.3. Individuals are also allowed to withdraw their consent (where this is not required for the Trust's legitimate interests) to the Trust's use of their Personal Data at any time. If a Trust employee receives such a withdrawal of consent, they must promptly inform the Data Protection Officer.

10.4. If anyone at the Trust receives a request to stop sending marketing materials, direct marketing communications of that type to that individual must be stopped as soon as is possible.

10.5. Individuals can also ask in writing for copies of their Personal Data which the Trust holds about them and other details about how the Trust uses their Personal Data.

10.6. Subject to receipt of proof of ID where considered necessary (and payment of any official fee permitted which the Trust has requested), following receipt of a written request from an individual for access to his/her Personal Data, the Trust will (to the extent requested by the individual):

(a) inform that individual whether the Trust holds Personal Data about him or her;
(b) describe the Personal Data about the individual which it holds, the reason for holding the Personal Data and the categories of persons to whom it may disclose the Personal Data; and
(c) provide the individual with copies of the Personal Data held about him or her, together with an indication of the source(s) of the Personal Data.

10.7. Strict rules must be followed as part of this process. Therefore, any such request received should be passed on to the Data Protection Officer. There are strict statutory deadlines for responding. Trust staff must not respond to any such request directly.

10.8. There is a right under the DPA known as "the right to be forgotten". This gives an individual the right to have their data erased when there is no compelling reason for continued processing. Under the DPA, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. Under the GDPR, this test is not present. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

11. Data Security

11.1. The Trust endeavours to keep all Personal Data secure by protecting data against being accessed by other companies or individuals (for example, via hacking), from being corrupted (data corruption) or being lost or stolen. This applies to Personal Data in IT systems, emails and attachments, and paper files.

11.2. For example, Trust staff [and School Contractors and volunteers where relevant] each have a password and individual controlled access rights to IT systems through their School computer and/or mobile or other electronic device.

11.3. Trust staff must comply with the School's security procedures whenever processing Personal Data. The Trust is dependent upon all employees to help keep Personal Data secure. Employees must only access and use Personal Data they are individually authorised to access and use and which is needed for a specific task within their School role.

11.4. Trust employees who work away from the School's premises must comply with any additional procedures and guidelines issued by the Trust for home working and/or offsite working. Extra care is needed to secure Personal Data in such cases, particularly Sensitive Personal Data. The following additional requirements apply:

- Do not access confidential information when you are in a public place, such as a train and may be overlooked;
- Do not have conversations about personal or confidential information on your mobile when in a public place. Ensure that, if urgent, you have your conversation in a separate room or away from other people;
- Remote log-in should be used so confidential documents do not have to be taken off side whenever possible so data is still being held securely on the Trust servers.
- If you use a laptop or tablet or smart phone:
    - Ensure that it is locked and password protected to prevent unauthorised access;
    - Make sure that you don't leave your device anywhere it could be stolen. Keep it with you at all times and secure it when you are in the Trust;
    - Portable devices or memory sticks that contain personal data must be encrypted. Personal data may not be taking off the Trust's site or put onto a portable device without the express permission of the Trust Head of ICT. Taking personal data off-site on a device or media that is not encrypted may be a disciplinary matter.
    - Ensure personal data is not stored on the hard drive;
- When working on confidential documents at home do not leave them lying around where others may see them; dispose of documents using a shredder.

11.5. The Trust also recognises that adequate security is important where it arranges for Third Parties to process Personal Data on its behalf, such as when outsourcing services to service providers, who process Personal Data on behalf of the Trust as a result ("a Data Processor"). The Trust remains liable for those service providers and their treatment of the Personal Data. The Trust will have suitable written contracts in place with such service providers with specific terms included to protect the Personal Data provided to them.

12. Disclosing Personal Data to Third Parties and Overseas Transfers

12.1. A disclosure of Personal Data is a form of processing. That means that the rules described above for fair and lawful use have to be satisfied. The Trust will not disclose Personal Data to a Third Party without first checking the disclosure is lawful and proportionate.

12.2. There are some exceptions to deal with disclosures, such as those requested lawfully by police where the information is necessary to prevent or detect a crime. Any request for Personal Data about an individual from government, police or other similar bodies or from journalists or other investigators should be passed immediately to the Data Protection Officer.

12.3. From time to time the Trust may pass pupil personal data (including sensitive personal data where appropriate) to third parties where lawful to do so, including local authorities, other public authorities, independent school bodies such as the Independent Schools Inspectorate and the Independent Schools Council, health professionals and the School's professional advisers, who will process the data:
- to enable the relevant authorities to monitor the School's performance;

- to compile statistical information (normally used on an anonymous basis);
- to secure funding for the School (and where relevant, on behalf of individual pupils); - to safeguard pupils' welfare and provide appropriate pastoral (and where relevant, medical and dental) care for pupils;
- where specifically requested by pupils and/or their parents or guardians;
- where necessary in connection with learning and extra-curricular activities undertaken by pupils;
- to enable pupils to take part in national and other assessments and to monitor pupils' progress and educational needs;
- to obtain appropriate professional advice and insurance for the Trust;
- where a reference or other information about a pupil or ex-pupil is requested by another educational establishment or employer to whom they have applied;
- otherwise where reasonably necessary for the operation of the School.

12.4. Unlawful disclosure (however well-meaning and however seemingly authoritative the requestor) risks placing the Trust in breach of several obligations under data protection legislation. Special care is needed with telephone requests for information, often used by unauthorised parties to 'blag' or obtain Personal Data to which they are not entitled. Trust employees must be certain of the identity of the person with whom they are dealing, ideally have a written request for information from them and ensure any disclosures are justified and authorised in advance.

12.5. There are special rules on whether Personal Data can be transferred to another country. Within the EU, there are restrictions on the transfer of Personal Data outside of the European Economic Area (EEA) (such a transfer can happen, for example, where Personal Data is emailed outside the EEA; where the School IT servers are hosted outside the EEA; or where there is remote on screen access from outside the EEA to Personal Data stored in an IT system within the EEA). This is to make sure the Personal Data remains safeguarded and that the individuals concerned do not lose the protection and rights they have under local law in respect of their Personal Data when transferred.

12.6. Actual or likely transfers of Personal Data to outside the EEA, especially of Sensitive Personal Data, should be clearly set out in the privacy notices described in the fair use section of this Policy (section 5) above so that such transfers are expected by the affected individuals.

13. Alumni, Marketing and Fundraising

13.1. As with other types of Processing, the use of Personal Data for marketing and fundraising purposes must satisfy the fair and lawful use requirements set out above. This means information notices must be given, and a lawful reason for processing has to be satisfied. Typically, this will have to be consent based.

13.2. Personal Data should not be used to contact individuals for marketing purposes by email, text or similar unless the individual has consented to marketing use. Individuals have a right to decline postal marketing and to object to any fundraising. Where marketing or fundraising is to be by phone, email, text or similar electronic means, normally individual consent is needed and must clearly cover marketing by that communication method. Special rules apply as to when consent is needed and how consent is obtained (for example, whether individuals can "opt out" of or "opt in" to receiving marketing) depending on the type of marketing contemplated and the means of communication with the individual. Any objections to marketing or requests to unsubscribe must be dealt with properly and promptly.

Appendix 1: Key Summary & Top Tips for Staff
Appendix 2: How we use your data - for Pupils and Parents

Appendix 1.

Key Summary and Top Tips for ("the Trust") Staff - Data Protection

Background

80% of data breaches involve staff within an organisation (figure from the Information Commissioner's Office) and breaches, for the most part, are unintentional. Therefore, everyone dealing with Personal Data needs to have a basic understanding of the Data Protection Act 1998 (DPA) and the new General Data Protection Directive (coming into force in 2018) that introduces more stringent data obligations.

The Trust collects a variety of personal data on students, parents, alumni, contractors, staff, volunteers, business contacts etc for legitimate business reasons in connection with the running of the Trust. It is vital that all this information is kept securely, is regularly reviewed and disposed of when no longer required.

Top Data Protection Tips:

1. Read and follow the Trust's Data Protection Policy.

2. Make sure all new staff within your department are aware of the Trust's policy and departmental procedures on data protection.

3. Use strong passwords on all devices and two step-authentication wherever possible. Ensure that any device you access school personal data on (mobiles for instance) are password protected.

4. It is preferable not to but if you must use portable memory devices, ensure these are encrypted (memory sticks, hard drives etc - the IT department can advise on this).

5. Do not download personal data onto personally owned devices unless absolutely necessary. In such cases, any personal data should be permanently deleted from the personal device as soon as is possible after use.

6. Only keep information as long as necessary - conduct periodic reviews (at least yearly) of personal systems (paper and electronic) and delete personal data that is no longer required.

7. If in any doubt about any personal data issue, contact the Trust's Data Protection lead.

Further Information:

Tips on keeping information secure:

- Keep passwords secure – change these regularly and do not share or give other people your password.
- Always lock &/or log off computers when away from your desk.
- Dispose of confidential paper waste by shredding.
- Prevent virus attacks by taking care when opening emails and attachments or visiting new websites.
- Hard copy personal information should be stored securely when it is not being used (lockable cabinets etc).

- Be careful when discussing individuals that you are not in earshot of anyone who does not need access to that information.
- Position computer screens away from windows and walkways to prevent accidental disclosures of personal information.
- Encrypt personal information that is being taken or sent outside the school or office.
- Do not, unless absolutely necessary, download personal data to a non-school device.

Tips on keeping only relevant information:

- Collect only the personal information required
- Explain new or changed business purposes to parents, pupils, employees and others, and obtain consent or provide an opt-out or opt-in where appropriate
- Update records promptly – for example, changes of address, phone numbers.
- Delete personal information the School no longer requires. If in doubt, please check whether the information should be retained. In the case of safeguarding information, this should always be passed to the Designated Safeguarding Lead for him to decide whether or not the information should be retained. Please make reference to the Trust's Data Retention Policy.
- Be aware that there may be people who will try and trick staff into giving out personal information.
- Carry out identity checks before giving out personal information to anyone in person, by writing or over the phone.

Handling requests from individuals for their personal information (subject access requests)

- People have a right to have a copy of the personal information the Trust holds.
- Any requests for Personal Data should be forwarded to the Trust's Data Protection lead.

Appendix 2.

Key Summary/Notice - How we use your information (for Pupils and Parents)

Background

For the purposes of Data Protection Law (the Data Protection Act 1998 and the General Data Protection Regulation) the Trust is the Data Controller of Personal Data about pupils and their parents and/or guardians (the School's Information Commissioner's registration details are listed in section 1 of the Trust's Data Protection Policy, published on the Trust's website).

In the main (unless otherwise specified), the Trust's basis for processing your and your child's personal data is legitimate interest - the Trust requires this information in order to run the School.

Personal Data processed by us includes:

- contact details;
- medical / health information;
- national curriculum and other assessment information;
- attendance records;
- information relating to special educational needs;
- images of pupils;
- in relation to parents and/or guardians - financial information.

We may also process Sensitive Personal Data (as defined earlier in this policy) such as information about parents' and / or pupils' ethnic group, religious beliefs and relevant medical information.

We acquire Personal Data in a number of ways. For example, parents of pupils may provide us with Personal Data about themselves or their family in correspondence, forms, documents, during discussions with staff, and through our website. Every form completed by a parent or child containing personal data will be held in accordance with the Trust's Data Protection Policy.

Data Check Form

Each academic year, a data check form is sent to parents and pupils (either electronically or in hard copy) that asks for personal data to be checked and data preferences to be updated. It is vitally important that this is completed by parents and pupils to ensure that the School maintains accurate records.

How we use your Personal Data

We commonly use Personal Data for:

- Ensuring that we provide a safe and secure environment;
- Making decisions relating to admissions, bursaries and scholarships (this may include video of your child)
- Providing pastoral care;
- Providing education and learning for children;
- Enabling pupils to take part in exams and assessments and to monitor and report on pupils' progress and educational needs;

- Providing additional activities for children and parents, such as extra-curricular clubs and educational trips and visits;
- Protecting and promoting our interests and objectives, including fundraising;
- Safeguarding and promoting the welfare of children;
- Where there has been a suspected misuse of the Trust's ICT facilities, investigating pupil's email communications and internet use; and
- Legal and management purposes and fulfilling our contractual and other legal obligations.

We may share Personal Data with third parties where doing so complies with the DPA. For example, we may share Personal Data:

- With relevant statutory agencies or authorities (e.g. for safeguarding reasons or in order to comply with our reporting obligations);
- Where necessary in connection with learning and extracurricular activities undertaken by pupils;
- When a reference or other information about a pupil or ex-pupil is requested by another educational establishment or employer to whom they have applied;
- To enable pupils to take part in national and other assessments;
- To obtain professional advice and insurance for the Trust; and/or
- Where otherwise required by law or where reasonably necessary for the operation of the School.
- We may share information about a pupil with their parents where permitted by the DPA, e.g. information about the pupil's academic attainment, behaviour and progress.

Biometric Information, Photographs & CCTV

Under the GDPR, biometric data is considered special category data and refers to the personal data about an individual's physical or behavioural characteristics which can be used to identify them, such as fingerprints or facial images. This data is collected and used as part of an automated biometric recognition system which can measure these characteristics to identify an individual.
An automated biometric recognition system processes data when:

- Recording pupils' biometric data, e.g. measuring fingerprints via a fingerprint scanner.
- Storing pupils' biometric data on a database.
- Using biometric data as part of an electronic process, e.g. by comparing it with data stored on a database to identify or recognise pupils.

Schools and colleges that use biometric data must comply with the requirements of the Protection of Freedoms Act 2012, and ensure the data is obtained, used and stored in accordance with the GDPR.

<u>Obtaining consent</u>
A school cannot lawfully process a pupil's biometric information without having obtained explicit consent from one of the persons detailed below.
The notification sent to parents should include information about the processing of their child's biometric information that is sufficient to ensure that parents are fully informed about what is being proposed. It should include:

- Details of the type of data required.
- How the data will be used.
- The parents' and pupil's right to refuse or withdraw consent.
- The school's duty to provide alternative arrangements for those whose information cannot be processed.

Unambiguous consent must always be used for biometric data usage – it must be freely given, specific and informed, and obtained on an opt-in basis. All parents of pupils under the age of 16, or 13 if the school determines them mature enough, must be notified for consent if the school wishes to take and use their child's biometric data as part of an automated biometric recognition system.

CCTV

We use CCTV recordings for the purposes of crime prevention and investigation and also in connection with our obligation to safeguard the welfare of pupils, staff and visitors to our site. CCTV recordings may be disclosed to third parties such as the police but only where such disclosure is in accordance with the DPA. Staff and pupils are also reminded that although the primary purpose of the School's CCTV system is the detection and prevention of crime, any evidence of misconduct captured incidentally on these cameras can be used as evidence in disciplinary matters. There will be no routine monitoring of data captured by CCTV for disciplinary purposes but in the event of an incident or allegation in relation to a visitor, pupil or member of staff, any existing footage may be reviewed if relevant to the allegations.

We may use photographs (and occasionally other media such as video or sound recordings) of pupils for educational purposes or in our publications, including on the school website and on social media, for marketing and promotion purposes. We may also share photographs and other media with third parties for these purposes (for example, for publication in a local or national newspaper). Consent will be sought for the use of photos in line with the Taking and Storing Images of Children Policy (available on the School website).

Data Retention

Personal data will be stored securely and not be kept for any longer than required for the Trust's legitimate purposes. Some records have to be retained for minimum periods by law. As a general rule, when personal data is no longer needed for the purposes for which it was collected, your data will be securely and permanently destroyed as soon as practicable.

The School, maintains a school archive of historical interest. This means that some data that is used for research purposes (and that is compatible with the purposes for which the data was originally collected) may be kept indefinitely if the relevant conditions apply.

For more information on the Trust's data retention policy or on how long it stores certain types of personal data, please contact the Trust's Data Protection lead.

Your Rights

You have rights in respect of your personal data and these are explained in the Trust's Data Protection Policy document. However, If you would like any further information please contact the Trust's Data Protection lead.