GST

Schools of Character
Making Great Leaders

DATA PROTECTION AND PRIVACY POLICY

Document Control

This document has been approved for use within	All GST Secondary Schools
This document has been approved by	Executive Leadership
On	Approval reported to the Board on 12.05.2022
Date effective from	16.05.2022
Date of next review	May 2024
Review period	Every 2 years
Status	Active
Owner	Data Protection Officer
Version	1.0

Contents

Rationale

We need student, parent and employee personal data to run our Trust and its schools successfully. We are trusted to look after this essential information. In order to operate effectively, we may also collect and use information relating to the people with whom we work, such as members of the public, contractors and suppliers. In addition, we may be required by law to collect and use information in order to comply with the requirements of central government.

Legal Framework

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

- the UK General Data Protection Regulation (UK GDPR);
- the Data Protection Act 2018 (DPA 2018);
- the Freedom of Information Act 2000;
- the Protection of Freedoms Act 2012 (when referring to our use of biometric data);
- the ICO's code of practice for the use of surveillance cameras and personal information; and
- our Funding Agreement and Articles of Association.

We are committed to ensuring that all personal data collected about staff, students, parents, Members of the Governance Team, visitors and other individuals is collected, stored and processed in accordance with the UK GDPR (the EU UK GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020) and the Data Protection Act 2018 (DPA 2018). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

We are committed to making every effort to meet our obligations under the UK GDPR legislation and will regularly review policies and procedures to ensure that we are doing so.

We recognise that each and every employee has a responsibility to comply with the appropriate data protection laws. Our schools and employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature. It is the responsibility of all members of the Trust community to take care when handling, using or transferring personal data so that it cannot be accessed by anyone who does not:

- have permission to access that data; and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and/or the school concerned, can bring the school and the Trust into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office (ICO). Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance.

The UK GDPR lays down a set of rules for processing of personal data (both structured manual records and digital records). The UK GDPR:

- defines what is meant by 'personal data';
- discusses rights on 'data subjects';
- places obligations on 'data controllers' and 'data processors';
- creates principles relating to the processing of personal data; and
- it provides for penalties for failure to comply with the above.

Personal Data

Under the UK GDPR, personal data is defined as:

"Any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified directly or indirectly, in particular by reference to 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."

The Six Principles of the UK GDPR

Under the UK GDPR, the data protection principles set out the main responsibilities for organisations. The UK GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Responsibilities

The UK GDPR requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

The Board of Trustees have overall responsibility for our compliance with the UK GDPR and have appointed a Data Protection Officer (DPO) to ensure compliance.

The Chief Executive Officer (CEO)/Chief Operating Strategic Officer ((COSO) referred to as Executive Leaders for the purpose of this policy) and Principals/Heads of School (HoS) are responsible for ensuring compliance with the UK GDPR and this policy within the day to day activities of the Trust and our schools. The Data Protection Officer (DPO) will have the support of Executive Leadership and Principals/Heads of School in order to ensure that appropriate training is provided for all staff.

Staff need to be aware of their obligations relating to any personal data they process as part of their duties. Any individual who knowingly or recklessly processes data for purposes other than those for which it is intended or makes an unauthorised disclosure is liable to disciplinary action and potentially criminal prosecution. Everyone has the responsibility of handling personal and sensitive personal data in a safe and secure manner.

The Trust and its schools will hold the minimum personal data necessary to enable them to perform their function and will not hold data for longer than necessary for the purposes it was collected for. Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

Data Controller

As a Multi Academy Trust (MAT), GST is responsible for the activities of all the schools in the MAT, even though some functions may have been delegated to Principals/HoS or Academy Councils. Ultimate responsibility lies with the MAT. GST is the legal entity responsible for the processing of personal data by the academies within the MAT, and therefore is the **data controller** subject to data protection obligations.

As a data controller, GST pays the appropriate Data Protection Fee to the Information Commissioner's Office on an annual basis and also provides contact details for our Data Protection Officer. The ICO publishes a register of fee-paying organisations which can be checked online by visiting: https://ico.org.uk/esdwebpages/search.

Board of Trustees and Academy Councils
The Board of Trustees and Academy Councils are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Trustee or Governor.

Data Protection Officer (DPO)
The UK GDPR makes it a requirement for public authorities to appoint a DPO. The UK GDPR defines the minimum tasks of the DPO as follows:

- to inform and advise the organisation and its employees about their obligations to comply with the UK GDPR and other data protection laws;
- to monitor compliance with the UK GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits; and
- to be the first point of contact for supervisory authorities and for individuals whose data is processed.

The DPO will operate independently reporting to the Trusts Executive Leaders will not be dismissed or penalised for performing their task and duties. The Trust will ensure that sufficient resources are provided to the DPO to enable them to meet their obligations.

Our current Data Protection Officer is Michelle Jones. You can contact our DPO and the supporting data protection team via email, on dpo@greatschoolstrust.com.

Accountability
GST will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR. We will provide comprehensive, clear and transparent privacy notices and as an employer with over 250 employees, additional internal records of our processing activities will be maintained and kept up-to-date. Internal records of processing activities will include 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; and
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.

GST will implement measures that meet the principles of data protection by design and data protection by default, such as:

- data minimisation;
- pseudonymisation;
- transparency;
- allowing individuals to monitor processing;
- continuously creating and improving security features; and
- use of data protection impact assessments, where appropriate.

Personal Data

The UK GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier (such as IP address).

The UK GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the UK GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive Personal Data

The UK GDPR has extended the definition of 'sensitive personal data' which requires even more protection than 'personal data'. Sensitive personal data includes data relating to the following:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data;
- health;
- sex life; and
- sexual orientation.

The Trust, our schools and our employees must be careful when handling sensitive personal data, especially if it's necessary to share it with other organisations, to ensure it is adequately protected at all times.

Lawful Processing

Under the UK GDPR, before any personal data is processed, the data controller has to identify what legal basis they are using to process the data and ensure that this is recorded. The UK GDPR sets out six legal bases that a data controller can consider and record before processing personal data:

- processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;
- processing is necessary for the **performance of a contract** with the data subject or to take steps to enter into a contract;
- processing is necessary for compliance with a **legal obligation**;
- processing is necessary to protect the **vital interests** of a data subject or another person;
- necessary 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. Note that this condition is not available to processing carried out by public authorities in the performance of their tasks; and
- **consent** of the data subject (or their parent/carer when appropriate in the case of a student).

If processing sensitive personal data, the UK GDPR sets out further legal bases that a data controller must consider and record before processing takes place:

- explicit consent of the data subject (or their parent/carer when appropriate in the case of a student);
- processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement;
- processing is necessary to protect the vital interests of a data subject or another individual where 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 or where courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards;
- processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional;

- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices; and
- processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- the individual (or their parent/carer when appropriate in the case of a student) has given consent;
- the data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent;
- the data has already been made manifestly public by the individual;
- the data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights;
- the data needs to be processed for reasons of substantial public interest as defined in legislation.

The majority of processing carried out by the Trust will be necessary for the performance of a task carried out in the public interest. As a public authority, it is in the public interest that the Trust operates schools and educates our children. Accordingly, for all the common tasks carried out by the Trust and our schools we do not need to ask for the data subject's consent but rather we can use public interest as our legal basis for processing the appropriate personal data.

This legal basis covers our use of personal data for all the everyday tasks within our schools such as:

- operating a curriculum;
- storing personal data about our students including their parental contacts;
- storing personal data about our staff;
- timetable information;
- cashless catering;
- library systems; and
- the annual census requirements.

However, there could well be some situations where the Trust might need to obtain explicit consent to process personal data or, at the very least, consider whether consent is needed. These could include situations where we share personal data with third party suppliers. If these are for everyday functions of a Trust/school that would be expected by any reasonable person, then 'public interest' may cover this processing. If, on the other hand, the third-party supplier is providing a service that might not be expected to be part of everyday school life, then explicit consent would be necessary.

Data Audit & Risk Register

A data audit and risk register will be maintained by the Data Protection Team with the support of Directors and Principals/Heads of School. Information Asset Owners (anyone responsible for the management or implementation of a system or the processing of data) will conduct information risk assessments to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- recognising the risks that are present;
- judging the level of the risks (both the likelihood and consequences); and
- prioritising the risks.

Risk assessments are an on-going process and will be securely saved on the GDPRis system.

Consent

Consent must be a positive indication and cannot be inferred from silence, inactivity or pre-ticked boxes. The Trust will only accept consent where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Where consent is given, a record will be kept documenting how and when consent was given. With regards to consent, please note:

- the Trust ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data will be found, or the processing will cease;
- consent previously accepted under the Data Protection Act (DPA) will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained;
- consent can be withdrawn by the individual at any time;
- where a student is under the age of 16, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a student; and
- if consent is our lawful basis for processing personal data when offering an online service directly to a child, only children aged 13 or over are able provide their own consent.

Individuals Rights

Data subjects (the living individual) that the personal data being processed relates to – have the following rights:

- **the right to be informed** – this means that individuals must be told what data we are using, why and for what purpose;
- **the right of access** – individuals have to be allowed to see what data of theirs we are processing if they request it;
- **the right of rectification** – if data is wrong, we have to correct it;
- **the right to erasure** – individuals can demand that all data of theirs be erased unless we have a legitimate legal basis for continuing to do so;
- **the right to restrict processing** – individuals can demand that we stop using their data unless we have a legitimate legal basis for continuing to do so;
- **the right to data portability** – individuals can decide to move their data to another processor and we have to provide them with all their data so they can do this, however, this only applies to data processed by automated means;
- **the right to object** – individuals can object to our use of their data and we must stop using it unless we have an overriding legitimate reason to continue; and
- **rights in relation to automated decision** - making or profiling – individuals can demand that automated decisions about them are reviewed by a human.

The Right to be Informed (Privacy Notice)

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

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;
- the 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 or 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; and
- the existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

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, as well as any possible consequences of failing to provide the personal data, will be provided. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained. In relation to data that is not obtained directly from the data subject, this information will be supplied:

- within one month of having obtained the data.
- if disclosure to another recipient is envisaged, at the latest, before the data is disclosed.
- if the data is used to communicate with the individual, at the latest, when the first communication takes place.

Information to Students and their Families – the "Privacy Notice"
In order to comply with our data protection obligations, we will inform students and parents/carers of all students of the data we collect, process and hold, the purposes for which the data is held, our legal basis for doing so, how long we will keep the data for and the third parties such as the Local Authority and Department for Education to whom it may be passed. This privacy notice will be passed to students and parents/carers through a specific letter and will be shared on the Trust/School websites. Parents/carers of new students to our schools will be provided with the privacy notice as part of the admissions process.

Information to the Workforce – the "Privacy Notice"
In order to comply with our data protection obligations, we will inform all staff of the data we collect, process and hold about them, the purposes for which the data is held, our legal basis for doing so, how long we will keep the data for and the third parties such as the Local Authority, Department for Education and HMRC to whom it may be passed. This privacy notice will be passed to staff through a specific letter. New staff joining our Trust will be provided with the privacy notice as part of their contract/induction process.

Our privacy notices can be found in Appendix A of this policy and on the Trust/school websites

The Right of Access (Data Subject Access Requests)

Individuals have the right to obtain confirmation that their data is being processed. Individuals also have the right to submit a Data Subject Access Request (DSAR) to gain access to their personal data in order to verify the lawfulness of the processing. A DSAR will provide the data subject with:

- confirmation that their personal data is being processed;
- access to a copy of the data;
- the purposes of the data processing;
- the categories of personal data concerned;
- who the data has been, or will be, shared with;
- how long the data will be stored for, or if this isn't possible, the criteria used to determine this period;
- the source of the data, if not the individual; and
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

When responding to a DSAR:

- we will verify the identity of the person making the request before any information is supplied;
- we may also contact the individual via phone to confirm the request was made;
- a copy of the information will be supplied to the individual free of charge; however, a 'reasonable fee' may be imposed to comply with requests for further copies of the same information;
- where a DSAR has been made electronically, the information will be provided in a commonly used electronic format;
- where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged;
- all fees will be based on the administrative cost of providing the information;
- all requests will be responded to without delay and at the latest, **within one calendar month** of receipt;
- 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;
- where a request is manifestly unfounded or excessive, the Trust 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; and

- in the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to.

When responding to a DSAR we will not disclose information if it:

- might cause serious harm to the physical or mental health of the student or another individual;
- would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- is contained in adoption or parental order records; or
- is given to a court in proceedings concerning the child.

Data Subject Access Requests should be submitted in writing, either by letter or email to the DPO. They should include:

- the name of the individual;
- the correspondence address;
- a contact number and email address; and
- details of the information requested

If staff receive a DSAR (verbally or in writing) they must immediately inform the DPO.

Children and Data Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Primary Schools: Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students below the age of 12 **may** be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Secondary Schools: Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students aged 12 and above **may not** be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Parental Requests to see the Educational Record

There is no automatic parental right of access to the educational record in academies and free schools. To request this, parents should make a Data Subject Access Request as set out above.

The Right to Rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where the personal data in question has been disclosed to third parties, we will inform them of the rectification where possible. Where appropriate, we will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex. Where no action is being taken in response to a request for rectification, we 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.

The Right to Erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. 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; and
- the personal data is processed in relation to the offer of information society services to a child.

We have 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; and
- the exercise or defence of legal claims.

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.

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

The Right to Restrict Processing

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

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.

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 we have 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; and
- where the Trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

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

Individuals will be informed when a restriction on processing has been lifted.

The Right to Data Portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. Personal data can be easily moved, copied or transferred from one ICT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies to personal data that an individual has provided to a controller where the processing is based on the individual's consent or for the performance of a contract and processing is carried out by automated means.

Personal data will be provided in a structured, commonly used and machine-readable form free of charge. Where feasible, data will be transmitted directly to another organisation at the request of the individual. We are not required to adopt or maintain processing systems which are technically compatible with other organisations.

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

We will respond to any requests for portability within one month. 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.

Where no action is being taken in response to a request, we 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.

The Right to Object

We 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.

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; and
- processing for purposes of scientific or historical research and statistics.

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; and
- we will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

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

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; and
- where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing of the data.

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

Automated Decision Making and Profiling

Individuals have the right not to be subject to a decision when:

- it is based on automated processing, e.g. profiling; and
- it produces a legal effect or a similarly significant effect on the individual.

We will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, we will ensure that the appropriate safeguards are in place, including:

- ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact;
- using appropriate mathematical or statistical procedures;
- implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors; and
- securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- we have the explicit consent of the individual; or
- the processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

Data Protection Impact Assessments (DPIAs)

We have adopted a privacy by design approach and are committed to implementing technical and organisational measures which demonstrate how we have considered and integrated data protection into our processing activities.

When planning to use new technologies and/or the processing is likely to result in a high risk to the rights and freedoms of individuals a Data Protection Impact Assessment (DPIA) will be carried out. DPIAs will be used to identify the most effective method of complying with our data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow us to identify and resolve problems at an early stage. Where it isn't clear whether a DPIA is required, our Data Protection Officer recommends that one is completed as it is a useful tool to help to ensure compliance with data protection law.

The following criteria should be considered when deciding whether a DPIA is needed. In most cases, meeting two criteria would require a DPIA, but a DPIA may still be completed for a processing operation meeting only one of these criteria. The criteria are:

- evaluation or scoring;
- automated decision making with legal or similar significant effect;
- systematic monitoring;
- sensitive data or data of a highly personal nature;
- data processed on a large scale;
- matching or combining datasets;
- data concerning vulnerable data subjects;
- innovative use or applying new technological or organisational solutions; and
- when the processing in itself prevents data subjects from exercising a right or using a service or contract.

Examples of high-risk processing include systematic and extensive processing activities, such as profiling, large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences and the use of CCTV.

We 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; and
- the measures implemented in order to address risk.

Data Breaches

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.

Principals and Senior Leadership Teams will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training. All staff members must ensure that suspected breaches are reported to our DPO immediately.

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

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it. 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.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, we will notify those concerned directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

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

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; and
- where appropriate, a description of the measures taken to mitigate any possible adverse effects.

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

Security

Security is paramount to all data processing throughout the Great Schools Trust and all staff are required to ensure that all personal/sensitive information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period:

- paper records containing personal/sensitive information must not be left unattended or in clear view anywhere with general access;
- paper records containing personal/sensitive information must be kept in a locked filing cabinet, drawer or safe, with restricted access;
- any personal/sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day;
- file cabinets containing personal/sensitive information must be kept closed and locked when not in use or when not attended;
- keys used for access to personal/sensitive information must not be left at an unattended desk;
- computer workstations must be locked when workspace is unoccupied;
- computer workstations must be shut completely down at the end of the work day;
- digital data stored on local hard drives and network drives are controlled by security access lists, and further encrypted or password-protected where necessary and are regularly backed up off-site;
- where data is saved on removable storage or a portable device (such as laptops and tablets), the device must be kept in a locked filing cabinet, drawer or safe when not in use;
- memory sticks must not be used to hold personal information unless they are password-protected and fully encrypted - data from our systems will only be writeable to Trust owned and encrypted USB memory sticks;
- all electronic devices are password-protected to protect the information on the device in case of theft;
- where possible, we enable electronic devices to allow the remote blocking or deletion of data in case of theft;
- staff will not use their personal laptops or computers for school purposes when processing personal data;
- all necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password;
- passwords must not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location;

- emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient;
- circular emails, (i.e. to parents) are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients;
- when sending confidential information by fax, staff will always check that the recipient is correct before sending;
- where personal/sensitive/confidential information 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 premises accepts full responsibility for the security of the data;
- before sharing data, all staff members will ensure:
    - that they are allowed to share it;
    - that adequate security is in place to protect it; and
    - that those who will be receiving the data have been outlined in a privacy notice.
- under no circumstances are visitors allowed access to personal/sensitive/confidential information;
- visitors to areas of the school containing sensitive information must be supervised at all times;
- printouts containing personal/sensitive information should be sent to the printer as a private print job and immediately removed from the printer upon release/printing;
- whiteboards containing personal/sensitive information should be erased;
- upon disposal personal/sensitive/confidential documents should be shredded
- the physical security of the school's buildings and storage systems, and access to them, is regularly reviewed. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place; and
- GST takes its Data Protection duties seriously and any unauthorised disclosure may result in disciplinary action.

Information Classification and Protective Marking

All Great Schools Trust information assets will be classified into one of the following three categories:

NOT PROTECTIVELY MARKED	OFFICIAL	OFFICIAL–SENSITIVE
Information that is published by the Trust, its schools, or made available to the public, or that is freely available.	The majority of information that is created or processed by the Trust and its schools, including that related to routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media.	A limited subset of OFFICIAL information that could have more damaging consequences (for individuals, the Trust or its schools) if it were lost, stolen or published in the media, where there is a clear and justifiable requirement to reinforce the "need to know".

These categories are explained in more detail below.

The classification NOT PROTECTIVELY MARKED

This applies only to information that rightly belongs in the public domain. This includes:

- information that the Trust / school publishes, for example on its website;
- other information that the Trust / school makes available to its community or members of the public, even though it does not routinely publish it;
- other information the Trust / school holds that is freely available.

There is no requirement to explicitly mark information with the classification NOT PROTECTIVELY MARKED.

The classification OFFICIAL

All routine business operations and services should be treated as OFFICIAL. The OFFICIAL classification covers information related to the following:

- the day to day business of the Trust / school, service delivery and public finances;
- safety, security and resilience;
- commercial interests, including information provided in confidence and intellectual property;
- individual people – personal information that must be protected under Data Protection legislation or other legislation (for example, health records).

The word OFFICIAL should be written in capital letters when it is being used as a term to classify information. There is no requirement to explicitly mark routine OFFICIAL information with its classification. However, it is acceptable to apply the label in particular circumstances if necessary.

The classification OFFICIAL–SENSITIVE

Some information which falls within the scope of the OFFICIAL classification may need a higher degree of protection than would normally be applied. This is given a stronger classification. The classification OFFICIAL–SENSITIVE applies when:

- there could be more serious consequences (for individuals, the Trust or its schools) in the event that the information is lost, stolen or published in the media; and
- there is a clear and justifiable requirement to restrict access solely to those who have a business need to know the information and who are within a trusted group.

The OFFICIAL–SENSITIVE classification covers the following:

- particularly sensitive information related to identifiable individuals, where inappropriate access could have damaging consequences (for example, information related to medical records, to investigations or to vulnerable individuals);
- commercially sensitive information (for example, related to contracts or financial matters);
- information that, if disclosed inappropriately, could compromise the operational effectiveness, internal stability or security of the Trust and its schools.

The OFFICIAL–SENSITIVE classification also applies to all information which is due to be destroyed.

The phrase OFFICIAL–SENSITIVE should be written in capital letters when it is being used as a term to classify information. Information classified as OFFICIAL–SENSITIVE must be clearly and obviously marked.

Further special labels for OFFICIAL–SENSITIVE information

Information in the OFFICIAL–SENSITIVE category may be further classified by one of two labels. In the Government Security Classifications document, these are called “descriptors”. These descriptors indicate the need for common sense precautions to limit access to the information. The two labels are as follows:

- In the case of particularly sensitive information related to identifiable individuals, the additional descriptor ‘PERSONAL’ may be applied. Such information would be marked as OFFICIAL–SENSITIVE [PERSONAL].
- In the case of commercially sensitive information, the additional descriptor ‘COMMERCIAL’ may be applied. Such information would be marked as OFFICIAL–SENSITIVE [COMMERCIAL].

The use of the descriptors is optional: all information classified as OFFICIAL–SENSITIVE must be labelled, but it is not mandatory to add one of the descriptors.

The descriptors should be written in capital letters and used only in conjunction with the OFFICIAL–SENSITIVE classification: they should never be used on their own or with any other classification.

Information combined from different sources

When information assets are gathered together from different sources, it may be the case that the individual items have different security classifications. In these cases, the overall collection of documents or files must carry the highest level of classification from the individual items. For example, if OFFICIAL–SENSITIVE information is combined with NOT PROTECTIVELY MARKED information, the overall collection of information would adopt the classification OFFICIAL–SENSITIVE and would need to be clearly marked to show that fact.

Additional guidance

Most student or staff personal data that is used within educational institutions will come under the OFFICIAL classification. However, some data e.g. the home address of a child at risk will be marked as OFFICIAL-SENSITIVE.

The Trust will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as OFFICIAL or higher.

When information is acquired or created, consideration must be given to how it should be classified.

All information classified as OFFICIAL–SENSITIVE must be clearly and obviously marked with its classification, and any additional descriptors (as described above) should be added if appropriate.

Consideration should be given to whether or not OFFICIAL information needs to be marked with its classification. For example, if it is considered necessary to draw attention to the fact that the information would not be expected to appear in the public domain, the OFFICIAL marking should be applied.

All documents (manual or digital) that are to be marked with a classification will be labelled clearly with the wording "DOCUMENT CONTROL:" in the footer accompanied by the appropriate classification, i.e. "DOCUMENT CONTROL: OFFICIAL-SENSITIVE".

Below are some examples of document control classifications for typical data processed in school.

Typical Information		**Document Control**
School life and events	School term times, holiday, training days, the curriculum, sports events and results, extracurricular activities, displays of students work, lunchtime menus, extended services, parent consultation, homework and resources, school prospectus.	Most of this information will fall into the NOT PROTECTIVELY MARKED category.
Learning and achievement	Information on how parents can support their individual child's learning, academic achievement, assessments, attainment, progress with learning, behaviour, IEPs.	Most of this information will fall into the OFFICIAL category. There may be learners whose personal data requires an OFFICIAL-SENSITIVE marking, e.g. the home address of a child at risk.
Safeguarding	Information pertinent to child protection issues.	Most of this information will fall into the OFFICIAL-SENSITIVE category, as it should only be accessed on a "need-to-know" basis.

Information must be stored securely in order to prevent unauthorised access. Stored information should be appropriately backed up to protect it against loss.

Access to information classified as OFFICIAL and OFFICIAL–SENSITIVE must be limited to those authorised to view it. Access must be granted only to those who require it in order to perform their jobs. OFFICIAL and OFFICIAL–SENSITIVE information must always be protected against unauthorised access. This means that users must be required to supply a user name and password, or equivalent, in order to gain access to the information.

Documents must also be securely destroyed after use, e.g. shredded. Destruction markings should also be included in the footer i.e. "Securely destroy after use".

Information that is protectively marked must keep its protective marking when it is printed, copied or transferred to portable media. Protectively marked information should be printed, copied or transferred to portable media only when necessary. All protectively marked information in portable form must be protected in transit and stored securely; it must not be left unattended without protection. For advice on encryption please contact a member of the ICT Team.

Below are some examples of different uses of technology and protective marking for typical data processed in school.

Typical Information		The Technology	Notes on Protect Markings
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of students work, lunchtime menus, extended services, parent consultation events.	Common practice is to use publicly accessible technology such as school websites or portal, emailed newsletters, subscription text services.	Most of this information will fall into the NOT PROTECTIVELY MARKED category.
Learning and achievement	Individual student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically, schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the OFFICIAL category. There may be students whose personal data requires an OFFICIAL-SENSITIVE marking. For example, the home address of a child at risk. In this case, the school may decide not to make this student record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via dashboards of information, or be used to provide further detail and context.	Most of this information will fall into the OFFICIAL category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts i.e. about school closures would fall into the NOT PROTECTIVELY MARKED category.

Publication of Information

We publish a publication scheme on our website outlining the classes of information that will be made routinely available, including:

- who we are and what we do;
- what we spend and how we spend it;
- what our priorities are and how we are doing;
- how we make decisions;
- our policies and procedures;
- lists and registers; and
- the services we offer.

Classes of information specified in the publication scheme are made available quickly and easily on request. For more information, please see the Trust Freedom of Information Policy & Publication Scheme.

We will not publish any personal information, including photos, on our website(s) without the permission of the affected individual. When uploading information to our website(s), staff are considerate of any metadata or deletions which could be accessed in documents and images on the site. For more information, please see the Trust School Information Published on a Website Policy.

Photographs and Videos

We understand that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. We will always indicate our intentions for taking photographs of students and will obtain written permission before publishing them.

Primary schools (students under 12): we will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and student.

Secondary schools (students over 12): we will obtain written consent from parents/carers, or students aged 16 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the images or video footage and not distribute them further.

Please see the Trust Online Safety Policy for more information on our use of photographs and videos.

Biometric Recognition Systems

Where we use students' biometric data as part of an automated biometric recognition system, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. We will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students.

Parents/carers and students can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

Where staff members or other adults use the biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and we will delete any relevant data already captured.

Please note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

More information about biometric data processing can be found in the **GST Biometric Data Protection Policy.**

CCTV

We use CCTV in various locations around our school sites to ensure that they remain safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. For more information, please see the Trust CCTV Policy and direct any enquiries regarding the CCTV systems to the Director of Capital Programmes, Estates and Facilities, via the school office.

Data Retention and Disposal

Personal data will not be kept for longer than is necessary and will be disposed of securely as soon as practicable. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on our behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Some educational records relating to former students or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

We have adopted the retention strategy of the Information Management Toolkit for Schools (pages 64-98) created by the IRMS (Information and Records Management Society) and adhere to its principles and guidance.

Training and Awareness

All staff will receive online data protection and privacy training and will be made aware of their responsibilities, as described in this policy through:

- induction training for new staff;
- annual staff training;
- staff meetings / briefings;
- day to day support and guidance from the DPO, the Directors and ICT Support.

Additional training will also be provided as part of continuing professional development, where changes to legislation, guidance or our own processes make it necessary.

Related Policies

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

- Trust Freedom of Information Policy & Publication Scheme;
- Trust Technical Security Policy;
- Trust Online Safety Policy;
- Trust Social Media Policy; and
- Trust Biometric Data Protection Policy

Monitoring and Review

The DPO is responsible for monitoring and reviewing this policy. It will be reviewed biannually or more regularly in the light of any significant new developments or in response to changes in guidance.

Appendix A: Privacy Notices

Please click on the relevant link below to access our privacy notices:

Student Privacy Notice
Parent/Carer Privacy Notice
Workforce Privacy Notice