University Schools Trust
A transformational education

Data Protection & Freedom of Information Policy

February 2023

Title:	Data Protection & Freedom of Information Policy
Procedure Code:	IO3.1
Source:	Specialist Redaction Services & UST
Document Owner:	Director of Data & Compliance
Review & Update By:	Director of Data & Compliance
Advisory Committee:	Audit & Risk Committee
Approval Committee:	Trust Board
Date Approved:	March 2023
Date of Publication:	March 2023
Date of Next Review:	February 2025
Required on Website:	Partial Requirement (Published all)

0. Document Control

The table below contains the changes made between the different final editions of this document set for approval. This is to help provide information to those reviewing and approving the document of the changes being made.

Document Edition	Section	Details of change
March 2023	5.8 and 8 18	Amendment to responsibilities and a new section regarding the requirement of Data Protection Impact Assessments Clarification regarding what constitutes a brecah in light of DfE guidance.
August 2022	All 0 1	Update to new brand Added Document Control Updated definitions for clarification

University Schools Trust
A transformational education

Contents

1. Definitions

The "Trust" refers to the company known as the University Schools Trust, East London and all Trustees, Governors and Staff who work within it.

A "School" refers to an individual academy within the Trust, as denoted by their Unique Reference Number. As such a 'school' may span one or several phases of education to the individual academies within the Trust. Depending on the context the term "School" may refer to a singular academy or to all of the academies within the Trust but as separate entities.

"Staff" refers to any individual who is employed by the Trust or who operates on the Trust's behalf, e.g. Trustees and Governors.

A "Parent" includes the natural or adoptive parent of a pupil as well as any non-parent / carer who has parental responsibility including being involved in the day-to-day care of a pupil.

A "Pupil" includes any incoming or current pupil at any School within the Trust. It also includes any individual who was previously a pupil at any School within the Trust and who has left within the appropriate timeframe for consideration as necessary, e.g. complaints. The term pupil is used as standard by the UST in its policy documents but can be replaced with the term "student" or "child" with no change of definition.

The "Headteacher" is defined as the individual who has ultimate responsibility for a school in line with UST strategy, approach, ethos and values. Individual schools may have alternative titles for this position such as Executive Headteacher or Principal.

The "Data Controller" is the UST. As such the UST is the organisation responsible for the implementation of this policy and for ensuring that the members of the UST adhere to the policy. The individual schools and sites within the UST are required to follow the principles and instructions outlined in this policy.

"Personal data" is information that identifies an individual and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain.

A sub-set of personal data is known as 'special category personal data'. This information is given special protection, and additional safeguards apply for this information to be collected and used. This special category data is information that relates to:

- race or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- physical or mental health;
- an individual's sex life or sexual orientation; and
- genetic or biometric data for the purpose of uniquely identifying a natural person.

Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

The UST does not intend to seek or hold sensitive personal data about staff or students except where the School has been notified of the information, or it comes to the school's attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or students are under no obligation to disclose to the school their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements).

The "Data Protection Officer" (DPO) refers to the individual / organisation that assist the Trust in the monitoring of internal compliance, informs and advises on data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the Information Commissioner. The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

2. Scope of the Policy

The UST collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the UST and/or the schools of the UST and as such applies to all of these individuals.

The General Data Protection Regulation (GDPR) applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

3. Policy Aims and Ethos

The Policy Aims and Ethos section is used to explain the purpose of the policy and what it seeks to achieve. It can also include any overarching principles that underpin the policy. An example from the admissions policy is shown here;
This policy aims to:

- Explain the University School's Trust (hereby referred to as either "the Trust" or "the UST") overall principles regarding admissions
- Set out each school's individual arrangements for allocating places to the pupils who apply
- Explain how to appeal against a decision not to offer your child a place

The Trust's overall principles for admissions are focussed on inclusivity and serving the local community of the schools. As part of this ethos, all schools within the Trust abide by the admissions arrangements of each individual school's Local Authority.

4. Links to Legislation and Guidance Documents

4.1. Relevant Internal Documents

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

- CCTV Policy
- Cookies Policy

- Freedom of Information Publication Document

4.2. Relevant External Documents

This policy has been created using the following external documents;

- Data Protection Act 2018
- The Information Commissioner's Office (ICO) Guide to the GDPR.

5. Roles and Responsibilities

5.1. Trust Board

The Trust Board;

- acts as Data Controller and therefore determines the determines the purposes for which and the manner in which any personal data are, or are to be processed;
- has responsibility for the content of this policy;
- has responsibility for ensuring that the policy is adhered to through delegated means;
- will review the policy as frequently as recommended by the Data Protection Officer (DPO);
- will ensure, through the DPO and the Policy Compliance Lead (PCL), that the policy is compliant with the regulations set out in the section above and that it reflects any changes as and when they occur;
- will ensure that appropriate measures are in place to enable the Trust to respond accurately and efficiently to Freedom of Information Requests (FOIs) and/or Subject Access Requests (SARs);
- will intervene through the Staff Disciplinary Process as and when required with respect to GDPR procedures;
- will appoint a Data Protection Champion for the Trust;
- will appoint an external Data Protection Officer to act on behalf of the Trust;
- will be aware of the scale and nature of all FOIs and SARs across the Trust; and
- will ensure that all Trust communications adhere to the GDPR regulations.

5.2. Local Governing Body

The LGB of each school;

- will be fully aware of the GDPR regulations;
- will ensure that their individual schools are GDPR compliant and adhere to this policy;
- will be aware of the scale and nature of FOI and SARs within their school; and
- will offer recommendations, as appropriate, to the Trust Board regarding necessary updates to the policy as a result of individual school circumstances.

5.3. Policy Compliance Lead (PCL)

The PCL is a Trust member of staff and will, as part of their role;

- ensure that this policy is distributed to the individual locations;
- ensure that all Trust staff are aware of the policy (including further revised editions); and
- make all necessary amendments to the policy following guidance from the DPO to ensure that it remains compliant with the aforementioned regulations.

5.4. Headteacher

The Headteacher will;

- appoint a Designated Policy Lead from among the senior staff;
- appoint a Data Protection Champion from among the senior staff;
- ensure that all staff receive policies as required; and
- ensure that all staff have access to all school and trust policies as required.

5.5. Designated Policy Lead (DPL)

- A DPL is a school-based member of staff in each school and will, as part of their role;
- ensure an accurate copy of this policy is available to all staff;
- disseminate updates regarding this and associated policies in a timely manner; and
- provide advice and guidance regarding the development of policies at the school level.

5.6. Data Protection Officer (DPO)

- In order to ensure that the defined requirements of the DPO are met, the Trust has engaged an external service to offer expert advice and resources to the Trust with respect to GDPR including FOIs and SARs. As part of this service the DPO will;
- conduct GDPR audits of each site within the Trust;
- provide training for all staff on GDPR;
- provide GDPR policy and Privacy Notice templates for adaptation;
- provide bespoke advice and guidance on any FOIs or SARs that affect either the Trust or a School within the Trust as necessary; and
- respond to FOIs and SARs, or where appropriate delegate responsibility to the Data Protection Champion.

5.7. Data Protection Champion (DPC)

A DPC (School) is appointed for each school. The UST Central office DPC will also undertake the role of Overall Trust DPC (Trust). The DPCs will;

- undertake training to be able to provide advice and guidance to colleagues within the school;
- work with the DPO to ensure that the areas for development from the audits are actioned in a timely and effective manner;
- be the initial point of contact for any location based GDPR queries, FOIs or SARs; and
- will liaise with the DPC (Trust) to ensure that all FOIs and SARs are logged within the school and within the Trust. The DPC (Trust) will liaise with the CEO.

5.8. All Staff

It is the responsibility of each member of staff to;

- ensure that they have read this policy and the associated documents;
- complete a Data Protection Impact Assessment (DPIA) if they are leading on a project involving the sharing of personal data
- attend GDPR training as required;
- act in accordance with this policy with respect to GDPR;
- report any data breaches to the DPC or a senior leader immediately and no later than one working day;

- report any FOIs or SARs to the DPC or a senior leader immediately and no later than one working day; and
- speak with their Line Manager or the DPL if they are uncertain regarding sections of any policy.

If a member of staff does not report a data incident (Data Breach, FOI, SAR) this could lead to disciplinary procedures. Following the guidance for GDPR, FOIs and SARs can be viewed as safeguarding personal data and should be treated with the same level of urgency that any other safeguarding matter would be.

If a member of staff has not raised that they did not understand a section of the policy, it may undermine their case should they be involved in an incident that breaches the school's / Trust's policies.

5.9. Other Stakeholders Including Pupils and Parents

There are a large number of other stakeholders that are associated with the individual schools and the Trust. It is the responsibility of other stakeholders (including pupils and parents) to;

- inform the school, in writing, of any limit or objection to the use of personal data; and
- raise any questions regarding data usage, in the broadest sense, with the school.

6. The Data Protection Principles (DPP)

The six data protection principles as laid down in the GDPR that must be followed at all times are;

- personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;
- personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;
- personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;
- personal data shall be accurate and, where necessary, kept up to date;
- personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes; and
- personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

In addition to this, the UST is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law.

The UST is committed to complying with the DPP at all times. This means that the Trust as an entity will;

- inform individuals as to the purpose of collecting any information from them, as and when we ask for it;
- be responsible for checking the quality and accuracy of the information;
- regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy;
- ensure that when information is authorised for disposal it is done appropriately;

- ensure appropriate security measures to safeguard personal information whether held in paper files or on our computer system, and follow the relevant security policy requirements at all times;
- share personal information with others only when it is necessary and legally appropriate to do so;
- set out clear procedures for responding to requests for access to personal information known as subject access requests; and
- report any breaches of the GDPR in accordance with the procedure within this policy.

7. Freedom of Information Publication Scheme

It is a requirement that the Trust have a Freedom of Information Publication Scheme. The scheme used is that provided by the ICO under the model publication scheme. This should be viewed in conjunction with the "Guide to Information Available" that can be found on the Trust website.
The link to the ICO model publication scheme can be found in Appendix 2.

8. Data Protection Impact Assessments (DPIA)

It is a requirement that any project or new software where the processing of personal data is likely to result in a "high risk to the rights and freedoms of individuals". The Trust uses the DPIA to assess that level of risk and then to also ensure appropriate mitigations are available before continuing with the project / software usage. As a result, the Trust will require the employed project lead to carry out a DPIA for any project / software that involves the sharing of any personal data.

9. International Transfers of Data

On occasion it may be required to send personal data outside of the EU. For example, this may be to institutions that students have applied to either as part of a transfer or as the next stage of their education. The Trust will seek to ensure every precaution is taken to check the validity of the request, the legitimacy of the destination and that the information is transferred in a secure manner.

10. Biometric Data

Students and their parents are notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent before we take any biometric data from their child and first process it.

Students and their parents have the right to choose not to use the Trust's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.
Where staff members or other adults use the school's 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.

At present the UST does, is a limited capacity, operate with some biometric data. This is limited to use with the cashless catering dinner system.

11. Approval Signature

Signature of (enter position e.g. Chair) _____

Print name _____

Date _____

12. Appendix 1 – Key Members of Staff Referenced

Role	Individual	Contact
Data Protection Officer (DPO)	Louise Manthorpe	specialistredactionservice@gmail.com
DPC UST (DPC Trust)	Darren Kulesza-Smith	dsmith@ust.london
DPC CJPS	Jesslyn Holman	Jesslyn.Holman@cyriljackson.towerhamlets.sch.uk
DPC RGTS	Ben Morgan	Morgan.B@rgtrustschool.net
DPC SPWT	Sultana Jeasmin	sjeasmin@spwt.net

13. Appendix 2 – Links to Legislation & Guidance

Data Protection Act 2018 https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

The Information Commissioner's Office (ICO) Guide to the GDPR can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

14. Appendix 3 – Applying the DPP within the UST

14.1. Processing Personal Data

The UST will adhere to the following conditions when processing personal data.

- The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given.
- The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.
- The processing is necessary for the performance of a legal obligation to which we are subject.
- The processing is necessary to protect the vital interests of the individual or another.
- The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us.

14.2. Use of Personal Data

The UST holds personal data on pupils, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the DPP as outlined previously.

14.2.1. Pupils

The personal data held regarding pupils includes;

- contact details;
- assessment / examination results;
- attendance information;
- characteristics such as ethnic group;
- special educational needs;
- any relevant medical information; and
- photographs.

The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, together with any other uses normally associated with this provision in a school environment.

The Trust may make use of limited personal data (such as contact details) relating to pupils, and their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the Trust Schools, but only where consent has been provided to this.

In particular, the UST may;

- transfer information to any association society club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to the Trust;
- make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities;
- keep the pupil's previous school informed of his / her academic progress and achievements e.g. sending a copy of the school reports for the pupil's first year at a school within the Trust to their previous school; or
- Use photographs of pupils in accordance with photography consent.

Any wish to limit or object to any use of personal data should be notified to the Data Protection Officer (DPO) in writing, which notice will be acknowledged in writing. If, in the view of the DPO the objection cannot be maintained, the individual will be given written reasons why the Trust cannot comply with their request.

14.2.2. Staff

The personal data held about staff will include;

- contact details,
- employment history,
- information relating to career progression,
- information relating to DBS checks,
- photographs.

The data is used to comply with legal obligations placed on the Trust in relation to employment, and the education of children in a school environment. The Trust may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

Any wish to limit or object to the uses to which personal data is to be put should be notified to the DPO who will ensure that this is recorded and adhered to if appropriate. If the DPO is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why it is not possible to comply with their request.

14.2.3. Other Individuals

The UST may hold personal information in relation to other individuals who have contact with the school, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles and shall not be kept longer than necessary.

14.3. Security of Personal Data

The UST will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the GDPR.

The UST will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

14.4. Disclosure of Personal Data to Third Parties

The following list includes the most usual reasons that the UST will authorise disclosure of personal data to a third party:

- to give a confidential reference relating to a current or former employee, volunteer or pupil;
- for the prevention or detection of crime;

- for the assessment of any tax or duty;
- where it is necessary to exercise a right or obligation conferred or imposed by law upon (other than an obligation imposed by contract);
- for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
- for the purpose of obtaining legal advice;
- for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);
- to publish the results of public examinations or other achievements of pupils of;
- to disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;
- to provide information to another educational establishment to which a pupil is transferring;
- to provide information to the Examination Authority as part of the examination process; and
- to provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

The Trust may receive requests from third parties (i.e. those other than the data subject, the Trust, and employees of the Trust) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or the Trust.

All requests for the disclosure of personal data must be sent to the DPO who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

14.5. Confidentiality of Pupil Concerns

Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, The Trust will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the Trust believes disclosure will be in the best interests of the pupil or other pupils.

14.6. Retention of Data

The UST follows the statutory guidance regarding retention of data as outlined in the Information and Records Management Society (IRMS) Retention Guidelines for Schools. The non-statutory guidance is followed as examples of best practice and adhered to wherever possible.
Appendix 3 should contain the procedures and processes associated with the policy if appropriate.

15. Appendix 4 - Rights of Individuals

The Trust has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how the UST will comply with the rights of individuals to;

- object to processing;
- object to rectification;
- object to erasure;
- object to data portability;
- raise a Subject Access Request (please see appendix 3); and
- raise a Freedom of Information Request (please see appendix 4).

15.1. Right to object to processing

An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest where they do not believe that those grounds are made out.

Where such an objection is made, it must be sent to the DPC within 1 working day of initial receipt, and to the DPO within 2 working days of initial receipt. The DPO will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

The DPO shall be responsible for notifying the individual of the outcome of their assessment within fourteen working days of receipt of the objection.

15.2. Right to rectification

An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it must be sent to the DPC within 1 working day of initial receipt, and to the DPO within 2 working days of initial receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified by the DPO.

Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given the option of a review under the data protection complaints procedure, or an appeal direct to the Information Commissioner.

An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

15.3. Right to erasure

Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances;

- where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
- where consent is withdrawn and there is no other legal basis for the processing;

- where an objection has been raised under the right to object, and found to be legitimate;
- where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met); or
- where there is a legal obligation for the UST to delete.

The DPO will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and/or has been made public, reasonable attempts to inform those controllers of the request shall be made.

The Trust has automatic erasure of CCTV imagery after 28 days with the exception for ongoing investigations. As such requests for the right to erasure for CCTV will not be upheld.

15.4. Right to restrict processing

In the following circumstances, processing of an individual's personal data may be restricted;

- where the accuracy of data has been contested, during the period when the Trust is attempting to verify the accuracy of the data;
- where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;
- where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim.

15.5. Right to portability

If an individual wishes to send their personal data to another organisation they have a right to request that the Trust provides their information in a structured, commonly used, and machine readable format.

As this right is limited to situations where the Trust is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If a request for this is made, it must be sent to the DPC within 1 working day of initial receipt, and to the DPO within 2 working days of initial receipt, and the DPO will review and revert as necessary.

16. Appendix 15 – Subject Access Requests (SARs)

Anybody who makes a request to see any personal information held about them by the Trust is making a SAR. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system".

The request, unlike a FOI, can be made via any medium and must be disclosed to the requestor within 28 days (It should be noted that for SARs the time requirements are not working days and are unaffected by school holidays and closures). All requests should be sent to the DPC within 1 working day of initial receipt, and to the DPO within 2 working days of initial receipt, and must be dealt with in full without delay and at the latest within one month of receipt.

Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The DPO must, however, be satisfied that;

- the child or young person lacks sufficient understanding; and
- the request made on behalf of the child or young person is in their interests.

All requests must have either the identity of the individual making the request verified.
In the case of the individual making the request for their own data a number of methods can be used to achieve this and include, but are not limited to;

- in person confirmation with a member of staff who knows the individual
- providing evidence confirming their identity, e.g. passport
- phone confirmation where knowledge is obtained that confirms the identity
- use of a known email account linked to that individual.

Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the Trust must have written evidence that the individual has authorised the person to make the application and the DPO must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected. Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

All files must be reviewed by the DPO before any disclosure takes place. Access will not be granted before this review has taken place.

16.1. Exemptions to Access by Data Subjects

Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

There are other exemptions from the right of subject access. If we intend to apply any of them to a request, then we will explain which exemption is being applied and why where appropriate.

17. Appendix 6 – Freedom of Information

The UST is subject to the Freedom of Information Act 2000 as a public authority, and as such, must comply with any requests for information in accordance with the principles laid out in the Act.

Any request for any information from the Trust is technically a request under the FOI Act, whether or not the individual making the request mentions the FOI Act. However, the ICO has stated that routine requests for information (such as a parent requesting a copy of a policy) can be dealt with outside of the provisions of the Act.

All requests should be referred in the first instance to the DPC within 1 working day of initial receipt and then to the DPO within 2 working days of initial receipt, who may allocate another individual to deal with the request.

When considering a request under FOI, you must bear in mind that release under FOI is treated as release to the general public, and so once it has been released to an individual, anyone can then access it, and you cannot restrict access when releasing by marking the information "confidential" or "restricted".

The Act only covers recorded information that is held or is easily accessible. Drawing on multiple sources of information to respond is usually deemed reasonable, however if the request is likely to require larger levels of manipulation this should be explained to the requestor as being prohibitive to the request. If the information is not held by the UST then it is not a requirement to find the information from an external source.

If the request is unclear or will require more that the recommended amount of time the UST, via the DPO, should inform the requestor of this and provide an opportunity for clarification from the requestor.

The UST must respond as soon as possible, and in any event, within 20 working days of the date of receipt of the request. When calculating the 20 working day deadline, a "working day" is a school day (one in which pupils are in attendance), subject to an absolute maximum of 60 normal working days (not school days) to respond.

When responding to a request where the Trust has withheld some or all of the information due to an exemption, the Trust must explain why the information has been withheld explaining how the information requested fits within that exemption. If the public interest test has been applied, this also needs to be explained.

The letter should end by explaining to the requestor how they can complain – either by reference to an internal review by a Board Trustee, or by writing to the ICO.

17.1. Refusing a FOI

The UST may decide to refuse a request. Common circumstances for refusing a FOI include;

- It would cost too much or take too much staff time to deal with the request*, however, the requestor should be notified of this in the response.
- The request is vexatious (likely to cause a disproportionate or unjustifiable level of distress, disruption or irritation).
- The request repeats a previous request from the same person.
- the request is for the applicant's personal data. This must be dealt with under the SARs process;
- compliance with the request would involve releasing third party personal data, and this would be in breach of the DPA principles as set out in paragraph 3.1 of the DPA policy above;
- information that has been sent to the UST (but not the Trust's own information) which is confidential;
- information that is already publicly available, even if payment of a fee is required to access that information;
- information that the Trust intends to publish at a future date;
- information that would prejudice the commercial interests of the Trust and / or a third party;
- information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information);
- information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras; or
- information which, in the opinion of the Chair of the Trust Board of the UST, would prejudice the effective conduct of the Trust. There is a special form for this on the ICO's website to assist with the obtaining of the chair's opinion.

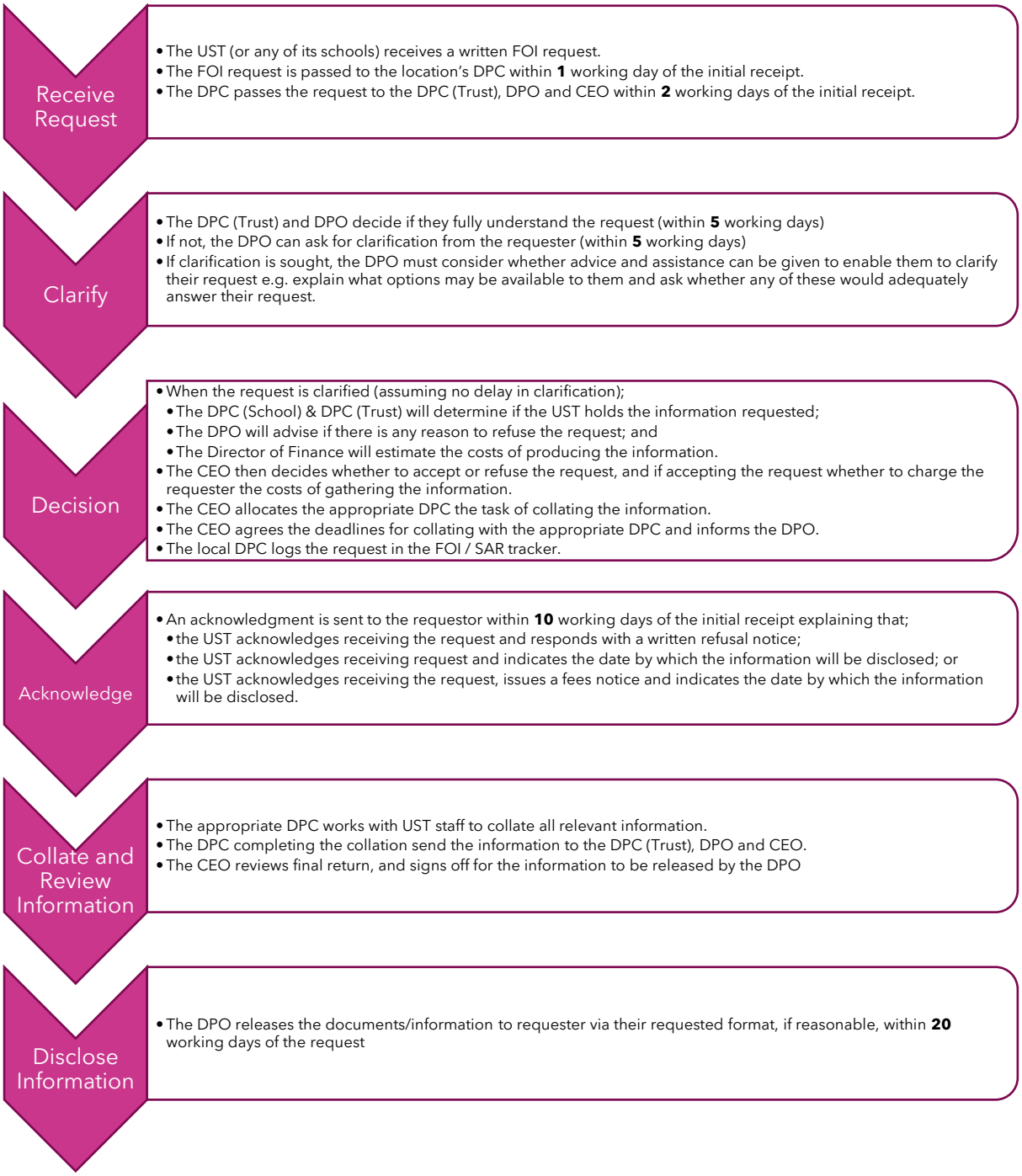
The sections mentioned in italics are qualified exemptions. This means that even if the exemption applies to the information, you also have to carry out a public interest weighting exercise, balancing the public interest in the information being released, as against the public interest in withholding the information.

*Information regarding limitations of FOIs relating to cost and /or resources

FOIs should not be allowed to cause a drain on time, energy and finances to the extent that they negatively affect the normal public functions. Currently, the cost limit for complying with a request or a linked series of requests from the same person or group is set at £600 for central government, Parliament and the armed forces and £450 for all other public authorities. Requests can be refused if it is estimated that the cost of compliance would exceed this limit. The biggest cost is likely to be staff time. Staff time should be rated at £25 per person per hour, regardless of who does the work, including external contractors. This means a limit of 18 staff hours.

17.2. Responding to a Freedom of Information Request

The following information summarises the basics of responding to FOI requests. For more detailed guidelines go to https://ico.org.uk/for-organisations/guide-to-freedom-of-information/



18. Appendix 7 – GDPR Breaches

Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the DCP who in turn shall report it to the DCP (Trust) DPO. At this point the DCP (Trust) will notify the CEO.
Once notified, the DPO shall assess:

- the extent of the breach;
- the risks to the data subjects as a consequence of the breach;
- any security measures in place that will protect the information; and
- any measures that can be taken immediately to mitigate the risk to the individuals.

Unless the DPO concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the UST, unless a delay can be justified.

The Information Commissioner shall be told via the ICO data breach form that includes information regarding;

- details of the breach;
- the volume of data at risk,
- the number of data subjects;
- the categories of data subjects;
- the contact point for any enquiries (usually the DPO);
- the likely consequences of the breach; and
- measures proposed or already taken to address the breach.

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the DPO shall notify data subjects of the breach via the DPCs without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Data subjects shall be told:

- the nature of the breach;
- who to contact with any questions; and
- measures taken to mitigate any risks.

The DPO shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Trust Board and a decision made about implementation of those recommendations.

For clarification a berach is considered to be where personal data is;

- Lost or stolen;
- Destroyed without consent;
- Changed without consent; and/or
- Accessed by someone without permission.

19. Appendix 8 – Privacy Notice for Pupils

Who processes your information?

The UST is the data controller of the personal information you provide to us. This means the Trust will determine the purposes for which, and the manner in which, any personal data relating to pupils and their families is to be processed. There may be times when it is necessary to share your personal data with a third party, this will only be done with your explicit consent, unless there is a legal requirement for the school to share your personal data.

Why do we collect and use your information?

The Trust has the legal right to collect and use personal data relating to pupils and their families, and we may also receive information regarding from your previous school, your LA (Local Authority) and the Department for Education (DfE).

We collect and use personal data in order to meet our legal requirements and legitimate interests as set out in the General Data Protection Regulations (GDPR) and UK law, including the following:

- Article 6 and Article 9 of the GDPR;
- Education Act 1996; and
- Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

In accordance with the above, the personal data of pupils and their families is collected and used for the following reasons;

- To support pupil learning;
- To monitor and report on pupil progress;
- To provide appropriate pastoral care;
- To assess the quality of our service;
- To comply with the law regarding data sharing;
- To safeguard pupils; and
- To communicate regarding the above.

What data is collected?

The categories of pupil information that the school collects, holds and shares may include;

- Personal information – e.g. names, pupil numbers and addresses;
- Characteristics – e.g. ethnicity, language, nationality and free school meal eligibility;
- Attendance information – e.g. number of absences and absence reasons;
- Assessment information – e.g. national curriculum assessment results;
- Relevant medical information;
- Information relating to SEND; and
- Behavioural information – e.g. number of temporary exclusions.

Whilst the majority of the personal data you provide to the school is mandatory, there may be some data that is provided on a voluntary basis. When we collect data from you we will inform you whether there is a mandatory requirement for you to provide this or whether your consent is required. When consent is required, the school will provide you detailed information with regards to the reasons the data is being collected and how the data will be used.

How long is your data stored for?

Personal data relating to pupils at schools within the UST and their families is stored in line with the school's GDPR Policy, specifically the section on Retention of Data. Data is only stored for as long as is necessary to complete the task for which it was originally collected.

Will my information be shared?

The school is required to share pupils' data with the DfE on a statutory basis.
The National Pupil Database (NPD) is managed by the DfE and contains information about pupils in schools in England. The Trust is required by law to provide information about our pupils to the DfE as part of statutory data collections, such as the school census; some of this information is then stored in the NPD. The DfE may share information about our pupils from the NDP with third parties who promote the education or wellbeing of children in England by;

- conducting research or analysis;
- producing statistics; and
- providing information, advice or guidance.

The Trust will not share your personal information with any third parties without your consent, unless the law permits us to do so. As well as the DfE, the school routinely shares pupils' information with:

- pupils' destinations upon leaving a Trust school;
- the Local Authority; and
- the NHS.

The school will also share information upon request where there is a legal requirement to do so such as with the police regarding a specific crime or potential crime.

The school will ensure that information will only be shared internally with staff where required for them to perform their professional duties.

What are your rights?

The parents / carers of pupils aged 12 and younger and pupils aged 13 or older have the following rights in relation to the processing of their personal data. You have the right to;

- be informed about how the Trust uses your personal data;
- request access to the personal data that the UST holds;
- request that your personal data is amended if it is inaccurate or incomplete;
- request that your personal data is erased when there is no reason for continued processing;
- request that the processing of your data is restricted; and
- object to your personal data being processed;

Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time.

If you have a concern about the way that the UST is collecting or using your personal data, you can raise a concern with the school / Trust as appropriate or if preferred with the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113 or for more information contact the DPO via email on specialistredactionservice@gmail.com.

20. Appendix 9 – Privacy Notice for Parents / Carers

Who processes your information?

The UST is the data controller of the personal information you provide to us. This means the Trust will determine the purposes for which, and the manner in which, any personal data relating to pupils and their families is to be processed. There may be times when it is necessary to share your personal data with a third party, this will only be done with your explicit consent, unless there is a legal requirement for the school to share your personal data.

Why do we collect and use your information?

The Trust has the legal right to collect and use personal data relating to pupils and their families, and we may also receive information regarding from your child's previous school, the LA (Local Authority) and the Department for Education (DfE).

We collect and use personal data in order to meet our legal requirements and legitimate interests as set out in the GDPR (General Data Protection Regulations) and UK law, including the following:

- Article 6 and Article 9 of the GDPR;
- Education Act 1996; and
- Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

In accordance with the above, the personal data of pupils and their families is collected and used for the following reasons;

- To support pupil learning;
- To monitor and report on pupil progress;
- To provide appropriate pastoral care;
- To assess the quality of our service;
- To comply with the law regarding data sharing; and
- To safeguard pupils; and
- To communicate regarding the above.

What data is collected?

The categories of information of parents / carers that the school collects, holds and shares may include;

- Personal information – e.g. names, pupil numbers and addresses;
- Characteristics – e.g. ethnicity, language, nationality and free school meal eligibility;
- Relevant medical information;
- Information relating to SEND; and
- Communications and interactions with the school – e.g. emails and telephone logs.

Whilst the majority of the personal data you provide to the school is mandatory, there may be some data that is provided on a voluntary basis. When we collect data from you, we will inform you whether there is a mandatory requirement for you to provide this or whether your consent is required. When consent is required, the school will provide you detailed information with regards to the reasons the data is being collected and how the data will be used.

How long is your data stored for?

Personal data relating to pupils at schools within the UST and their families is stored in line with the school's GDPR Policy, specifically the section on Retention of Data. Data is only stored for as long as is necessary to complete the task for which it was originally collected.

Will my information be shared?

The school is required to share pupils' data with the DfE on a statutory basis.
The National Pupil Database (NPD) is managed by the DfE and contains information about pupils in schools in England. The Trust is required by law to provide information about our pupils to the DfE as part of statutory data collections, such as the school census; some of this information is then stored in the NPD. The DfE may share information about our pupils from the NDP with third parties who promote the education or wellbeing of children in England by;

- conducting research or analysis;
- producing statistics; and
- providing information, advice or guidance.

The Trust will not share your personal information with any third parties without your consent, unless the law permits us to do so. As well as the DfE, the school routinely shares information with:

- pupils' destinations upon leaving a Trust school;
- the Local Authority; and
- the NHS.

The school will also share information upon request where there is a legal requirement to do so such as with the police regarding a specific crime or potential crime.

The school will ensure that information will only be shared internally with staff where required for them to perform their professional duties.

What are your rights?

All parents/carers have the following rights in relation to the processing of their own personal data and those of their children if they are 12 or younger. Under those conditions you have the right to;

- be informed about how the Trust uses your personal data;
- request access to the personal data that the Trust holds;
- request that your personal data is amended if it is inaccurate or incomplete;
- request that your personal data is erased where there is no reason for its continued processing;
- request that the processing of your data is restricted; and
- object to your personal data being processed.

Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time.

If you have a concern about the way that the UST is collecting or using your personal data, you can raise a concern with the school / Trust as appropriate or if preferred with the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113 or for more information contact the DPO via email on specialistredactionservice@gmail.com.

21. Appendix 10 – Privacy Notice for Staff

Who processes your information?

The UST is the data controller and as such processes personal data relating to those we employ to work at, or otherwise engage to work at any part of the Trust. This includes contractors and agency staff as appropriate. This is for employment purposes such as to assist in the running of the Trust and / or to enable individuals to be paid.

How will we use your information?

This personal data includes identifiers such as names and national insurance numbers, employment contracts and remuneration details, qualifications and absence information. It will also include sensitive personal data such as ethnic group, medical information and trade union membership (if you choose to supply this information to us).

During the recruitment process we may receive information about you from a previous employer or an educational establishment which you have previously attended. You will know about this because you will have supplied us with the relevant contact details.

Collecting and using your information in this way is lawful because;

- the processing is necessary for the performance of your employment contract;
- the processing is necessary for the performance of a legal obligation to which BCCFS is subject, for example our legal duty to safeguard pupils;
- the processing is necessary to protect the vital interests of others, i.e. to protect pupils from harm; and
- the processing is necessary for the performance of our education function which is a function in the public interest.

When we collect personal information, we will make it clear whether there is a legal requirement for you to provide it, and whether there is a legal requirement on the school to collect it. If there is no legal requirement then we will explain why we need it and what the consequences are if it is not provided.

Will your information be shared?

The UST will not share information about you with third parties without your consent unless the law permits us to. We are required, by law, to pass on some of the personal data which we collect to the appropriate local authority and the Department for Education (DfE).

The collection of this information will benefit both national and local users by;

- improving the management of workforce data across the sector;
- enabling development of a comprehensive picture of the workforce and how it is deployed;
- informing the development of recruitment and retention policies;
- allowing better financial modelling and planning;
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body.

We disclose personal data about you to the Disclosure and Barring Service for the purposes of carrying out checks on your suitability for work with children.

We disclose details about you including national insurance number and absence information to our payroll provider to enable you to be paid.

We disclose details about you to our HR provider for the purposes of HR management.

We share your identity and pay information with HMRC in conjunction with your legal obligation to pay income tax and make national insurance contributions.

We share your details with your pension provider in order to make sure that you pay the correct amount and maintain your entitlement to a pension upon your retirement. For teachers the scheme is the TPS, for support staff the scheme is LGPS.

Our disclosures to third parties are lawful because one of the following reasons applies;

- The disclosure is necessary for the performance of your employment contract;
- The disclosure is necessary for the performance of a legal obligation to which the Academy Trust is subject, for example our legal duty to safeguard pupils;
- The disclosure is necessary to protect the vital interests of others; or
- The disclosure is necessary for the performance of our education function which is a function in the public interest.

The school will ensure that information will only be shared internally with staff where required for them to perform their professional duties.

How long is your data stored for?

The Trust only keep your information for as long as we need it or for as long as we are required by law to keep it. Further details can be found in the main body of the GDPR policy.

What are your rights?

You have the right to:

- request access to your personal information;
- request rectification of the information we hold about you;
- request the erasure of information about you;
- request that our processing of your personal information to be restricted;
- request data portability; and
- object to us processing your information.

For any of the above please contact the School's or Trust's Data Protection Champion (as appropriate) or the Trust's Data Protection Officer (DPO).

If at any time you are not happy with how we are processing your personal information, then you may raise the issue with the Director of Data and Compliance or if preferred the DPO who can be contacted on specialistredactionservice@gmail.com. If you are not happy with the outcome you may raise a complaint with the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113.

22. Appendix 11 - Privacy Notice for Governance Individuals

Who processes your information?

The UST is the data controller of the personal information you provide to us. This means the Trust will determine the purposes for which, and the manner in which, any personal data relating to pupils and their families is to be processed. There may be times when it is necessary to share your personal data with a third party, this will only be done with your explicit consent, unless there is a legal requirement for the school to share your personal data.

Why do we collect and use your information?

The Trust collects your personal data to help us run the school by:

- Establishing and maintaining effective governance;
- Meeting our statutory obligations for publishing and sharing details;
- Facilitating safe recruitment, as part of our safeguarding obligations towards pupils;
- Undertaking equalities monitoring; and
- Ensuring that appropriate access arrangements can be provided if required.

Which data is collected?

The categories of Governor, Trustee and Member information that the school collects, holds and shares include the following:

- Contact details;
- References;
- Evidence of qualifications
- Employment details
- Information about business and pecuniary interests

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This may include information about (where applicable):

- Race;
- Ethnicity;
- Religious beliefs;
- Sexual orientation;
- Political opinions; and
- Disability and access requirements.

How long is your data stored for?

Personal data relating to Governors of the UST is stored in line with the school's GDPR Policy.
In accordance with the GDPR, the school does not store personal data indefinitely and data is only stored for as long as is necessary to complete the task for which it was originally collected.

Will my information be shared?

The Trust will not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with Data Protection law) we may share personal information about you with:

- Government departments or agencies – to meet our legal obligations to share information about governors/trustees;
- Our local authority – to meet our legal obligations to share certain information with it, such as details of governors;
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as governor/trustee support;
- Professional advisers and consultants;
- Employment and recruitment agencies; or
- Police forces and the courts.

What are your rights?

Governors, Trustees and Members have the following rights in relation to the processing of their personal data.

You have the right to:

- Be informed about how the Trust uses your personal data;
- Request access to the personal data that the Trust holds;
- Request that your personal data is amended if it is inaccurate or incomplete;
- Request that your personal data is erased where there is no compelling reason for its continued processing;
- Request that the processing of your data is restricted; and
- Object to your personal data being processed.

Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time.

If at any time you are not happy with how we are processing your personal information then you may raise the issue with the Director of Data and Compliance or if preferred the DPO who can be contacted on specialistredactionservice@gmail.com. If you are not happy with the outcome you may raise a complaint with the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113.

23. Appendix 12 – Privacy Notice for Visitors

The UST is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

What information will we collect?

We will collect, store, and use the following categories of personal information about you;

- Personal details including name, car registration and the organisation you are visiting from; and
- Information about your visit, including the date and time it occurred, and who you were visiting.

We will not collect or store any sensitive personal data about you.

How is your personal information collected?

We collect personal information about our Visitors through the on-site electronic registration mechanism or, in the event of the electronic registration system being unavailable, a visitor's registration log book.

How will we use information about you?

Situations in which we will use your personal information;

- We use your personal information to ensure your safety and wellbeing when you visit our premises;
- We will use the information to make direct contact with you regarding the work relationship between the Trust and you or your organisation; and
- We will use the information to make direct contact with you regarding future opportunities with the UST

How long will you use my information for?

The Trust only keep your information for as long as we need it or for as long as we are required by law to keep it. Further details can be found in the main body of the GDPR policy.

What are your rights?

You have the right to:

- request access to your personal information;
- request rectification of the information we hold about you;
- request the erasure of information about you;
- request that our processing of your personal information to be restricted;
- request data portability; and
- object to us processing your information.

If you have a concern about the way that the UST is collecting or using your personal data, you can raise a concern with the school / Trust as appropriate or if preferred with the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113 or for more information contact the DPO via email on specialistredactionservice@gmail.com.

24. Appendix 13 – Data Protection Overview Guidance for Staff

Data protection and data security is the responsibility of every member of staff who processes personal information. Please read and comply with the following guidance:

- Staff should always be clear about why they are processing data and should not process any personal information other than in accordance with the terms and conditions of the Schools Data Protection Policy.
- Staff may not process personal data without the individual's consent, unless there is a legitimate reason for doing so without consent.
- Parents/ Carers and Students have a legal right to access their personal information therefore staff should be accurate and measured in what they record.
- Other than in the case of approved routine data transfers (e.g. DofE/ National Pupil Database/ Onward Education Establishment) staff should not disclose personal information to external third parties without obtaining consent from the individual, or unless permitted to do so by law. If you are unsure, please contact the School Data Protection Officer.
- Email addresses are personal data. Do not send emails (e.g. to large numbers of recipients) showing the private email addresses of all the recipients. For confidentiality please blind copy the addressees and send the email to yourself when sending such emails.
- Keep secure all files containing personal data whether on paper or on computer.
- Apply password protection to computers, screensavers and documents. Where possible keep your office door locked and your desk clear of personal data when you are absent
- All paper based personal information should be locked away at night.
- Laptops, other portable equipment containing personal data, computer should be locked up at night.
- Memory Sticks must not be used for transferring personal data.
- Email attachments containing personal data must be by secure mail.
- If individuals disclose sensitive data/information, for instance about their health, ensure that it is stored securely and revealed only to those members of staff who need to know it.
- Confidential waste must always be shredded, and not put into a waste or recycling bin.

Data Breaches: All data breaches (accidental disclosures/losses of personal data) must be reported immediately to the local Data Protection Champion, the Data Protection Officer (at specialistredactionservice@gmail.com) and the Headteacher as soon as the breach has been discovered so that appropriate measures can be taken to recover the data and limit any damage.

The school is obliged to report serious breaches to the Information Commissioner.