Unity Schools Trust

'Excellence through collaboration'

Data Protection & Freedom of Rights Policy

Policy Reviewed:	June 2018
Next Review:	June 2019
Approved by Trust	to be confirmed

Contents

1. Aims

Within the Trust we hold personal data on staff, students, parents, governors and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined below. The Trust aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

This policy meets the requirements of the GDPR. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. The 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.

Biometric Data

This policy meets the requirements of the 1) Protection of Freedoms Act 2012 when referring to our use of biometric data and 2) Consent for the General Data Protection Regulation (GDPR) 2018 Compliance.

CCTV

This policy also reflects the ICO's code of practice for the use of surveillance cameras and personal information (See Appendix 2).

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • name (including initials) • identification number • location data • online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
The Trust	The Unity Schools Trust and any schools that are members of the Trust
Personal data breach	Any event leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

The Trust processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and Responsibilities

This policy applies to **all staff** employed within the Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trustees

The Trustees have overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

5.2 Data Protection Officer (DPO)

The DPO is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is *Mrs Rnuka Dhir* and is contactable at dataprotection@unityschoolstrust.co.uk.

5.3 Head of School/Business Director & Chief Financial Officer

The Head of School, or their designate, and the Business Director & Chief Financial Officer act as the representative of the data controller on a day-to-day basis.

5.4 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not, they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data Protection Principles

The GDPR is based on data protection principles that our Trust, and the schools within, must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;
- Collected for specified, explicit and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;
- Adequate, relevant and limited to what is necessary to fulfil the purpose(s) for which it is processed;
- Accurate and, where necessary, kept up to date;
- Kept for no longer than is necessary for the purpose(s) for which it is processed
- Processed in such a way that ensures it is appropriate security of data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

The Trust is committed to complying with these principles at all times. This means that the Trust will:

- Inform individuals about how and why we process their data through the privacy notices that we issue;
- 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 guidelines as advised in the "Information and Records Management Society's Toolkit for Schools";
- Ensure that when information is authorised for disposal it is done appropriately;
- Ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer systems, and follow the relevant security procedure 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;
- Report any breaches of the GDPR in accordance with the procedure in Appendix 1.

7. Collecting Personal Data

7.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have one of the following 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed so that the Trust can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life

- The data needs to be processed so that the Trust, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR.

If we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student is under thirteen years of age (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

Staff must only process personal data where it is necessary in order to do their jobs.
When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's Toolkit for Schools.

7.3 Use of Student and Staff Personal Data by the Trust

Students

The personal data held regarding students 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 students, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the Trust as a whole is doing, together with any other uses normally associated with this provision in a school environment.

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

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

In particular, the Trust may:

- Transfer information to any association society or club set up for the purpose of maintaining contact with students or for fundraising, marketing or promotional purposes relating to the Trust but only where consent has been obtained first;
- Make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities;

- Keep the student's previous school informed of his/her academic progress and achievements e.g. sending a copy of the school reports for the student's first year at the Trust to their previous school;
- Use photographs of students in accordance with the photograph policy.

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

Staff

The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks, photographs and occupational pensions.

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.

Information Relating to DBS Checks

DBS checks are carried out on the basis of the Trust's legal obligations in relation to the safer recruitment of staff as stipulated in the Independent School Standards Regulations and DBS Information (which will include personal data relating to criminal convictions and offences) is further processes in the substantial public interest, with the objective of safeguarding children. Retention of the information is followed by using the guidelines provided by "Information and Records Management Society's Toolkit for Schools".

Access to the DBS information is restricted to those staff who have a genuine need to have access to it for their job roles. In addition to the provisions of the GDPR and the Data Protection Act 2018, disclosure of this information is restricted by section 124 of the police Act 1997 and disclosure to third parties will only be made if it is determined to be lawful.

Any wish to limit or object to the uses to which personal data is to be put should be notified to the Data Protection Officer who will ensure that this is recorded, and adhered to if appropriate. If the Data Protection Officer 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 the Trust cannot comply with their request.

Other Individuals

The Trust 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 in accordance with the data protection principles, and shall not be kept longer than necessary.

8. Sharing Personal Data - Disclosure of Personal Data to Third Parties

We will not normally share personal data with anyone else, but may do so:

- Where there is an issue with a student or parent/carer that puts the safety of our staff at risk
- To give a confidential reference relating to a current or former employee, volunteer or student
- To provide information to another educational establishment to which a student is transferring
- For the purpose of obtaining legal advice
- To publish the results of public examinations or other achievements of students within the Trust
- To disclose details of a student's medical condition where it is in the student's interest to do so, for example for medical advice, insurance purposes or to organisers of school trips; The legal basis will vary in each case but will usually be based on explicit consent, the vital interests of the child or reasons of substantial public interest (usually safeguarding the child or other individuals)
- To provide information to the Examination Authority as part of the examination process
- Where we need to liaise with other agencies – we will seek consent as necessary before doing this
- If our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided
- 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 of Education (DfE). The examination authority may also pass information to the DfE.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

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 students cannot be identified from them. On occasion the DfE may share the personal data with the 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 and employees of the Trust) to disclose personal data it holds about students 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 Business Director & Chief Financial Officer, *Mrs Liz Simmons* (dataprotection@unityschools.co.uk), 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.

Confidentiality of Student Concerns

Where a student seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents and guardian, the Trust will maintain confidentiality unless it has reasonable grounds to believe that the student does not fully understand the consequences of withholding their consent, or where the Trust believes disclosure will be in the best interests of the student or other students. Disclosure for a safeguarding purpose will be lawful because it will be in the substantial public interest.

Please see the Child Protection Policy of individual schools for more details that are available on their website.

9. Subject Access Requests and Other Rights of Individuals

9.1 Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust holds about them. This includes:

- 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
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should be submitted in writing, either by letter or email the DPO. They should include:

- Name of individual
- Correspondence address

- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO, and must be dealt with in full without delay and at latest within one month of receipt.

9.2 Children and 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.

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 within our Trust 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 by the Head of School.

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 Head of School must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

9.3 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or voluminous. We will inform the individual of this within one month, and explain why the extension is necessary

We will not disclose information in instances where there are exemptions, such as:

- 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
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to appeal to the ICO.

A subject access request must be made in writing. The Trust may ask for any further information reasonably required to locate the information.

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 information. Particular care must be taken in the case of any complaint or dispute to ensure confidentially is protected.

All files must be reviewed by the Business Director & Financial Chief Officer before any disclosure takes place. Access will not be granted before this review has taken place.
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.

9.4 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parent/Carer Requests to See the Educational Record

Parent/carers do not have an automatic right of access to the educational record of their child as the schools within the Trust are academies, but we may choose to provide this. This decision will be at the discretion of the Head of School and/or Business Director & Chief Financial Officer.

11. Biometric Recognition Systems

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

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012 and Consent for the General Data Protection Regulation (GDPR) 2018 Compliance.

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

Parent/carers and students 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 students.

Parent/carers and students can object to participation in the Trust's biometric recognition system(s), or 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/carers.

Where staff members or other adults use the Trust'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. Staff and other adults can also withdraw consent at any time, and the Trust will delete any relevant data already captured.

See Appendix 2 for more details about Biometric Recognition Systems.

12. CCTV

We use CCTV in various locations around the Trust to ensure it remains 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 prominent signs are displayed explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Head of IT & Network Services, *Mr Ben Wakefield,* at dataprotection@unityschoolstrust.co.uk.

Please see Appendix 3 for more details about the CCTV management procedures.

13. Photographs and Videos

As part of our Trust activities, we may take photographs and record images of individuals within the Trust.

We will obtain written consent from parent/carers and students 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. The school

will not normally seek consent for any internal use of photographs as the processing of such personal data is in accordance with the statutory functions of the school in providing an education to the student and is therefore lawful on the grounds of public interest. However, the school will take into account any parental preferences expressed. The student may also exercise their data protection rights in respect of photographs and videos as set out in our Data Protection and Freedom of Rights Policy. We will respond appropriately to any student or parental request to exercise those rights. Uses may include:

- Within school on notice and video boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on school websites or social media pages

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

When using photographs and videos in this way we will not accompany them with any other personal information about the child.

See Appendix 4, Photograph and Video Procedure, for more information on our use of photographs and videos.

14. Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly communicating with members of staff on data protection law, this policy, any related policies and any other data protection matters
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Trust and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data Security and Storage of Records

All staff will be made aware of this Policy and their duties under the GDPR. We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date, where we cannot or do not need to rectify or update it, will also be disposed of securely. 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 the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal Data Breaches

The Trust will make all reasonable endeavors to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within seventy-two hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of students eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about students

18. Training

All staff and governors are provided with guidance and information on data protection as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. Freedom of Information

The Trust is subject to the Freedom of Information Act 2000 (FOI) 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 information from the Trust is technically a request under the FOI, whether or not the individual making the request mentions the FOI. 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.

In all non-routine cases, if the request is simple and the information is to be released, then the individual who received the request can release the information, but must ensure that this is done within the timescale set out below. A copy of the request and response should then be sent to the Business Director & Chief Financial Officer.

All other requests should be referred in the first instance to the Business Director & Chief Financial Officer, who may allocate another individual to deal with the request. This must be done promptly, and in any event within three working days of receiving the request.

When considering a request under FOI, it should be borne 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 Trust must respond as soon as possible, and in any event, within twenty working days of the date of receipt of the request. For the Trust, a "working day" when calculating the twenty working day deadline, a "working day" is a school day (one in which students are in attendance), subject to an absolute maximum of sixty normal working days (not school days) to respond.

Full details about the procedure for management of a FOI request can be found at Appendix 5.

Any questions about the Freedom of Rights in this policy should be directed in the first instance to the DPO.

20. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

Appendix 1: Personal Data Breach Procedure

The DPO shall 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 Trustees and a decision made about the implementation of those recommendations.

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO

- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people

- The DPO will alert the Head of School, Business Director, CEO and the Chair of Trustees

- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

    If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trusts' computer system.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the Trusts' secure computer system.
The DPO and Head of School will meet to review what happened and how future breaches can be prevented. This meeting will happen as soon as reasonably possible.

Actions to Minimise the Impact of Data Breaches

The Trust will take the appropriate actions to mitigate the impact of different types of data breach. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Actions for Sensitive Data

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Appendix 2: Biometric Recognition System

Biometric recognition systems

The typical uses of biometrics in school are those where the student puts their finger or thumb into a machine as a means of identification e.g. cashless catering and library borrowing books. New data protection legislation has come into force in the UK. This legislation impacts on how student's biometric data should be processed. Due to the effect of this change we must obtain consent from every child who has capacity (generally from year 7 onwards) who is going to use the system. Where there are students who do not have sufficient understanding to give their own consent, a parent/carer with responsibility for the student should consent on their behalf: Consent is required for both 1) Protection of Freedom Act 2012 **and** 2) Consent for the GDPR Compliance to satisfy the requirements of both laws.

1) Protection of Freedom Act 2012

Where we use students biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash) we will comply with the requirements of the Protection of Freedoms Act 2012.

For existing students, you will already have given your permission for us to use your biometric data. However, given the changes in data protection, we are seeking renewed permission to use your data. For new students, please note this is notification to parents/carers before any biometric recognition system is put in place or before their child first takes part in it. As a school we are asking for 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 object to participation in the school's biometric recognition system(s), or 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).

2) Consent for the General Data Protection Regulation (GDPR) 2018 Compliance

The provisions in the Protection of Freedoms Act 2012 are in addition to the requirements under the GDPR with which schools must continue to comply.

When processing a student's personal data, including biometric data for the purposes of an automated biometric recognition system, as a school we comply with the GDPR key data protection principles.

This means, for example, we will:

- Store biometric data securely to prevent any unauthorised or unlawful use.
- Not keep biometric data for longer than it is needed meaning that we will destroy a student's biometric data if, for whatever reason, the student no longer uses the system including when he or she leaves the school or where a parent withdraws consent or the student objects.

- Ensure that biometric data is used only for the purposes for which they are obtained and that such data are not unlawfully disclosed to third parties. For further information about the data protection principles and complying with the GDPR 2018 please see our Data Protection and Freedom of Rights Policy, available to down load from our school website.

Declaration – Biometrics Recognition Systems

- I have received and read the Biometrics recognition systems information provided by the school.
- I understand that the typical uses are where the student puts their finger or thumb in the machine as a means for identification e.g. cashless catering and borrowing books.
- I understand that even if there is consent, a student/parent/carer can object or refuse at any time to the student's biometric information being taken/used. Any relevant data already captured will be deleted.
- I understand that students and parents/carers have the right to choose not to use the school's biometric system(s). The school will provide alternative means of accessing the relevant services for those students.
- I understand that when the student leaves the school their biometric data will be securely deleted.
- I consent to Biometric recognition systems being used on the legal basis of the "Protection of Freedom Act 2012" and "Consent for the General Data Protection Regulation (GDPR) 2018 Compliance".

Parent/Carer Name: _____

Parent/Carer Signature: _____

Date: _____

Student Name: _____

Student Signature: _____

Date: _____

Appendix 3: Procedure for the Management of CCTV

1 Introduction

1.1 The Trust uses closed circuit television (CCTV) and the images produced to prevent or detect crime and to monitor school buildings and grounds in order to provide a safe and secure environment for its students, staff and visitors, and to prevent loss or damage to Trust property.

1.2 The system comprises a number of fixed and dome cameras.

1.3 The system does have sound recording capability in some areas.

1.4 The CCTV system is owned and operated by the Trust, the deployment of which is determined by the Head of IT and Network Services and Head of School in each school.

1.5 CCTV is monitored centrally by IT & Network Services as well as a number of nominated senior staff having controlled access. A register of users authorised to access CCTV is maintained by the Head of IT and Network Services.

1.6 The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and members of the school community.

1.7 The Trusts' CCTV Scheme is registered with the ICO under the terms of the GDPR. The use of CCTV, and the associated images are covered by the GDPR. This procedure outlines the Trust's use of CCTV and how it complies with the Act.

1.8 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. Through this procedure, all operators are made aware of their responsibilities in following the CCTV Code of Practice. The Trust will ensure that all employees are aware of the restrictions in relation to access to, and disclosure of, recorded images by publication of this policy.

2 Statement of Intent

2.1 The Trust's usage complies with the ICO CCTV Code of Practice, ensuring CCTV is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at:

https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

2.2 CCTV warning signs are clearly and prominently placed at the main external entrances to the schools, including further signage where appropriate. Signs will contain details of the purpose for using CCTV. In areas where CCTV is used, the Trust will ensure that there are prominent signs placed within the controlled area.

2.3 The original planning, design and installation of CCTV equipment endeavoured to ensure that the scheme will deliver maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3 Siting the Cameras

3.1 Cameras are sited so that they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The Trust will ensure that the location of equipment is carefully considered to ensure that images captured comply with the GDPR.

3.2 The Trust will make every effort to position cameras so that their coverage is restricted to the school premises, which includes outdoor/indoor areas.

3.3 CCTV may be used in classrooms and in limited areas within the school building that have been identified by staff and students as not being easily monitored at all times.

3.4 Members of staff will have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

4 Covert Monitoring

4.1 It is not the Trust's policy to conduct 'Covert Monitoring' unless there are exceptional reasons for doing so.

4.2 The Trust may, in exceptional circumstances, determine a sound reason to set up covert monitoring. For example:

- Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

4.3 In these circumstances authorisation must be obtained from the Business Director & Chief Financial Officer and Head of School advised before any commencement of such covert monitoring.

4.4 Covert monitoring must cease following completion of an investigation.

4.5 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilet cubicles, changing areas etc.

5 Storage and Retention of CCTV Images

5.1 Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

5.2 All retained data will be stored securely at all times and permanently deleted as appropriate/required.

6 Enquiries

Enquiries about the operation of CCTV within the school should be directed to the Head of IT and Network Services, Mr Ben Wakefield at dataprotection@unityschoolstrust.co.uk.

7 Further Information

Further information on CCTV and its use is available from the following:

- CCTV Code of Practice Revised Edition 2017 (published by the Information Commissioners Office) Version 1.2
- www.ico.org.uk
- Regulation of Investigatory Powers Act (RIPA) 2000

8 CCTV Signage

It is a requirement of the GDPR to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The Trust will ensure that this requirement is fulfilled.

The CCTV sign should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The name of the school
- The contact details for any enquiries

Checklist

This CCTV system and the images produced by it are controlled by senior IT & Network Services staff who are responsible for how the system is used under direction from the Trust/school. The Trust/school notifies the Information Commissioner about the CCTV system, including any modifications of use and/or its purpose, as required by the GDPR. The Trust/school has considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of the school's community. It will not be used for other purposes. The school will conduct regular reviews of our use of CCTV.

	Date checked	**Name (person checking)**	**Date of next review**
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			
There is a named individual who is responsible for the operation of the system.			
A system had been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.			
Staff and members of the school community will be consulted about any proposal to install / amend CCTV equipment or its use as appropriate.			
Cameras have been sited so that they provide clear images.			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be			
Except for law enforcement bodies, images will not be provided to third parties.			
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the data controller knows to seek advice from the Information Commissioner as soon as such a request is made.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

Appendix 4: Photograph and Video Procedure

The Trust is obliged to comply with the GDPR when it takes or publishes photographs of its students. The Trust will always try to act in the best interest of the students and, as far as it legally can, it will take parental preferences into account.

The school will not normally seek consent for any internal use of photographs as the processing of such personal data is in accordance with the statutory functions of the school in providing an education to the student and is therefore lawful on the grounds of public interest. However, the school will take into account any parental preferences expressed. The student may also exercise their data protection rights in respect of photographs and videos as set out in this Policy. We will respond appropriately to any student or parental request to exercise those rights.

The Data Protection Act gives children rights over their own data when they are considered to have adequate capacity to understand. Most children will reach this level of understanding at around age 12. For this reason, for most students in a secondary school it will normally be up to the individual child to decide whether or not to be photographed. Where the Trust considers that the child does not have the capacity to make such a decision the Trust will act as it considers to be in the best interests of the child and in doing so will take account of any stated parental preference.

If a parent/carer wishes to express a preference for the Trust to avoid taking or publishing photographs of a child in certain circumstances, then they should indicate their preferences using the form located at Appendix 3.1. If no preferences are expressed, then the Trust will act in accordance with the principles expressed in this policy. Consent can be refused or withdrawn at any time. If consent is withdrawn, the Trust will delete the photograph or video and not distribute it further.

Ordinarily the following rules will apply to photographs in this Trust:

Photographs for Internal Use

- The Trust will take photographs for its own use. Usually these will be unnamed photographs and will generally be for internal Trust use but may also include photographs for publication, such as photos for the prospectus, or to show as slides at an event for parents. Unnamed photographs may also be used on display and video boards which can be seen by visitors to the Trust.
- When the photograph is taken, the students will be informed that a photograph is being taken and told what it is for so that they can object if they wish.
- If the Trust wants to use named photographs, then it will obtain specific consent first. For most students this will be student consent as explained above but parental wishes will be taken into account.

School Website

The Trust will only use photographs of students on the school website with consent. This consent must be the consent of the child when the child has sufficient understanding to make the decision for themselves (generally age 12 onwards) but the Trust will take into account any parental preferences expressed and so will not ordinarily publish against the wishes of parents. In cases where both parents of the child cannot agree but the child is consenting, the Trust will

make a decision based on the best interests of the child, after careful consideration of the circumstances and after having taken legal advice.

Media Use

- The Trust will give proper consideration to the interests of its students when deciding whether to allow external organisations to take photographs or to film.
- When the Media are allowed to be present in school or at school events, this will be on the condition that they observe this policy.
- Where the media are allowed to be present at a particular event the Trust will make sure that students and their parents or carers are informed of the media presence. If no objection is received, then the Trust will assume that unnamed photographs may be published.
- If the Media entity wants to publish named photographs, then they must obtain specific consent from those students with capacity to consent or the parents of those without capacity. The Trust will require the media entity to check with the Trust before publication so that the Trust can check that any objections have been taken into account.

Family Photographs at Trust Events

- It shall be at the discretion of the Trust whether photographs may be taken at a school event.
- Family and friends taking photographs for the family album will not be covered by Data Protection legislation.
- Where the Trust decides to allow such photography, the family and friends will be asked not to publish any photographs showing children other than their own on the internet.

Appendix 4.1

Photographic Images of Student - Consent form

Student name:

Student class:

To comply with the General Data Protection Regulations 2018, we need your permission to photograph or make any recording of you (student)/your child.

The table below shows the different ways you (student)/your child's image/name may be used. Please tick to confirm your consent or otherwise for each medium, sign and date the form and return it to your school office as soon as possible.

What	Where	Yes	No
Student image and name	In school *e.g. display boards*		
Student name or image *Unidentifiable by full name and photograph combined unless agreed in advance with an adult with parental responsibility*	School publications *e.g. newsletter, DVD*		
Student name or image *Unidentifiable by full name unless agreed in advance with an adult with parental responsibility*	School online publications *e.g. website, app*		
Student image *Without name*	School social media *e.g. Facebook*		
Student being photographed or filmed *News media may publish pictures along with the student's full name, but the Trust will seek an undertaking that a student's name will not be used if their image is put on the newspaper's own website.*	External press/media *e.g. newspapers, television images*		
Student being photographed or filmed at school fixtures and events *We may use the pictures for our school publications and/or on our website. We may also make video or web cam recordings for use by the Trust.*	School publications *e.g. prospectus, newsletters, website*		

Photographic Images of Student - Declaration

I have read and understood the consent asked of me above. My decision on whether to give consent will remain valid throughout my/my child's time in my/their current key stage, unless I notify the school of the contrary in writing. I promise that if I, or members of my family, take photographs or video recordings at a school event, these will be kept for family use only and will not be uploaded to social media.

Parent/Carer Name: _____

Parent/Carer Signature: _____

Date: _____

Student Name: _____

Student Signature: _____

Date: _____

Appendix 5: Procedure for Dealing with a Freedom of Information Request

When a request is received that cannot be dealt with by simply providing the information, it should be referred in the first instance to the Business Director & Chief Financial Officer, who may re-allocate to an individual with responsibility for the type of information requested.

1.1 The first stage in responding is to determine whether or not the Trust "holds" the information requested. The Trust will hold the information if it exists in computer or paper format. Some requests will require the Trust to take information from different sources and manipulate it in some way. Where this would take minimal effort, the Trust is considered to "hold" that information, but if the required manipulation would take a significant amount of time, the requestor should be contacted to explain that the information is not held in the manner requested, and offered the opportunity to refine their request. For example, if a request required the Trust to add up totals in a spread sheet and release the total figures, this would be information "held" by the Trust. If the Trust would have to go through a number of spread sheets and identify individual figures and provide a total, this is likely not to be information "held" by the Trust, depending on the time involved in extracting the information.

1.2 The second stage is to decide whether the information can be released, or whether one of the exemptions set out in the Act applies to the information. Common exemptions that might apply include:

1.2.1 Section 40 (1) – the request is for the applicants' personal data. This must be dealt with under the subject access regime above;
1.2.2 Section 40 (2) – compliance with the request would involve releasing third party personal data, and this would be in breach of the DPA principles as set out above;
1.2.3 Section 41 – information that has been sent to the Trust (but not the Trust's own information) which is confidential;
1.2.4 Section 21 – information that is already publicly available, even if payment of a fee is required to access that information;
1.2.5 Section 22 – information that the Trust intends to publish at a future date;
1.2.6 Section 43 – information that would prejudice the commercial interests of the Trust and / or a third party;
1.2.7 Section 38 – information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information);
1.2.8 Section 31 – information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras;
1.2.9 Section 36 – information which, in the opinion of the Chair of the Trust, 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.

1.3 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.

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

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