Policy Approved:	**January 2025**
Next Review:	**December 2026**
Effective Date:	**January 2025**

Contents:

Appendices:

1.0 **Aims**

1.1 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 Data Protection, Privacy and Electronic Communications (Ammendments etc) (EU Exit) Regulations 2019 and the Data Protection Act 2018 (DPA 2018).

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

2.0 **Legislation and Guidance**

2.1 This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR. 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.

2.2 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.

2.3 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.

3.0 **Definitions**

Term	Definition
Personal data	Any information relating to an 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 • Child protection safeguarding as set out in page 10
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.

4.0 **The Data Controller**

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

4.2 The Trust is registered with the ICO/has paid its data protection fee to the ICO, as legally required.

5.0 **Roles and Responsibilities**

This policy applies to **all staff** employed within the Trust, and to external organisations or voluntary workers and 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 reports 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 contactable at dataprotection@unityschools.co.uk .

5.3 Principal / CEO

The Principal, or their designate, and the CEO act as the representative of the data controller on a day-to-day basis.

5.4 All Staff

Staff are responsible for:

5.4.1 Collecting, storing and processing any personal data in accordance with this policy

5.4.2 Informing the school of any changes to their personal data, such as a change of address

5.4.3 Contacting the DPO in the following circumstances:

i. With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
ii. If they have any concerns that this policy is not being followed
iii. If they are unsure whether or not, they have a lawful basis to use personal data in a particular way
iv. 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 of the UK
v. If there has been a data breach
vi. Whenever they are engaging in a new activity that may affect the privacy rights of individuals
vii. If they need help with any contracts or sharing personal data with third parties

6.0 **Data Protection Principles**

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

6.1 The principles say that personal data must be:

6.1.1 Processed lawfully, fairly and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;

6.1.2 Collected for specified, explicit and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;

6.1.3 Adequate, relevant and limited to what is necessary to fulfil the purpose(s) for which it is processed;

6.1.4 Accurate and, where necessary, kept up to date;

6.1.5 Kept for no longer than is necessary for the purpose(s) for which it is processed;

6.1.6 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:

6.2 6.2.1 Inform individuals about how and why we process their data through the privacy notices that we issue;

6.2.2 Be responsible for checking the quality and accuracy of the information;

6.2.3 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";

6.2.4 Ensure that when information is authorised for disposal it is done appropriately;

6.2.5 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;

6.2.6 Share personal information with others only when it is necessary and legally appropriate to do so;

6.2.7 Set out clear procedures for responding to requests for access to personal information known as subject access requests;

6.2.8 Report any breaches of the GDPR in accordance with the procedure in Appendix 1.

7.0 Collecting Personal Data

7.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have one of the following 6 'lawful bases' (legal reasons) to do so under data protection law:

7.1.1 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

7.1.2 The data needs to be processed so that the Trust can **comply with a legal obligation**

7.1.3 The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life

7.1.4 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**

7.1.5 The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.

7.1.6 The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent**

7.2 For special categories of personal data, we will also meet one of the special category conditions for processing under the data protection law:

7.2.1 The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**

7.2.2 The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**

7.2.3 The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent

7.2.4 The data has already been made **manifestly public** by the individual

7.2.5 The data needs to be processed for the establishment, exercise or defence of **legal claims**

7.2.6 The data needs to be processed for reasons of **substantial public interest** as defined in legislation

7.2.7 The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law

7.2.8 The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law

7.2.9 The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

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

7.3.1 The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**

7.3.2 The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent

7.3.3 The data has already been made **manifestly public** by the individual

7.3.4 The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**

7.3.5 The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.4 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.

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.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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.

7.5 Use of Student and Staff Personal Data by the Trust

7.5.1 Students

i. 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.
ii. 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.
iii. 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.
iv. 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.

7.5.2 In particular, the Trust may:

i. 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;
ii. Make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities;
iii. 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;
iv. 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

7.6

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

7.7

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

7.8

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.

8.0 **Sharing Personal Data - Disclosure of Personal Data to Third Parties**

8.1 Due regard will be given to relevant data protection principles, which allows us to share (and withhold) personal information, as provided for in the Data Protection Act 2018 and the GDPR. We will not normally share personal data with anyone else, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

8.1.1 Where there is an issue with a student or parent/carer that puts the safety of our staff at risk

8.1.2 To give a confidential reference relating to a current or former employee, volunteer or student

8.1.3 To provide information to another educational establishment to which a student is transferring

8.1.4 For the purpose of obtaining legal advice
8.1.5 To publish the results of public examinations or other achievements of students within the Trust
8.1.6 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)
8.1.7 To provide information to the Examination Authority as part of the examination process
8.1.8 Where we need to liaise with other agencies – we will seek consent as necessary before doing this
8.1.9 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:

i. Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
ii. 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
iii. 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.

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.

'Safeguarding of children and individuals at risk' is a processing condition that allows us to share special category personal data. Information may be shared without consent where there is good reason to do so, and that the sharing of information will enhance the safeguarding of a child in a timely manner but it is not possible to gain consent, it cannot be reasonably expected to gain consent, or if to gain consent would place a child at risk.

We will not provide students' personal data where the serious harm test under the legislation is met. For example, in a situation where a child is in a refuge or another form of emergency accommodation, and the serious harms test is met, we will withhold providing the data in compliance with the schools' obligations under the Data Protection Act 2018 and the GDPR.

Where we transfer personal data to a country or territory outside of the UK, 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 DPO (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.

8.2 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 Safeguarding and Child Protection Policy of individual schools for more details that are available on their website.

9.0 Subject Access Requests and Other Rights of Individuals

9.1 Subject Access Requests

9.1.1 Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust holds about them. This includes, but is not limited to:

i. Confirmation that their personal data is being processed
ii. Access to a copy of the data
iii. The purposes of the data processing
iv. The categories of personal data concerned
v. Who the data has been, or will be, shared with
vi. How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
vii. Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
viii. The right to lodge a complaint with the ICO or another supervisory authority
ix. The source of the data, if not the individual
x. Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
xi. The safeguards provided if the data is being transferred internationally

9.1.2 Subject access requests must be submitted in writing, either by letter or email the DPO on dataprotection@unityschools.co.uk. They should include:

i. Name of individual
ii. Correspondence address
iii. Contact number and email address
iv. Details of the information requested

We may be able to respond to requests more swiftly if they are made using our Subject Access Request form (see Appendix 2).

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 Principal.

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 Principal 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

9.3.1 When responding to requests, we:

i. May ask the individual to provide two forms of identification
ii. May contact the individual via phone to confirm the request was made
iii. Will respond without delay and within one month of receipt of the request
iv. Will provide the information free of charge
v. 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.

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

i. Might cause serious harm to the physical or mental health of the student or another individual
ii. 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
iii. Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it (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).
iv. Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.
If a subject access request is made the Trust may ask for any further information reasonably required to locate the information.

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

9.4 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.

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:

i. Withdraw their consent to processing at any time
ii. Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
iii. Prevent use of their personal data for direct marketing
iv. Challenge processing which has been justified on the basis of public interest
v. Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
vi. Be notified of a data breach in certain circumstances
vii. Make a complaint to the ICO
viii. 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.

10.0 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 Principal and/or CEO.

11.0 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 3 for more details about Biometric Recognition Systems.

12.0 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 IT & Network Services Manager at cto@unityschools.co.uk.

Please see Appendix 4 for more details about the CCTV management procedures.

13.0 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.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or students where appropriate) have agreed to this.

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 Policy. We will respond appropriately to any student or parental request to exercise those rights. Where the school takes photographs and videos uses may include:

i. Within school on notice and video boards and in school magazines, brochures, newsletters, etc.
ii. Outside of school by external agencies such as the school photographer, newspapers, campaigns
iii. 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, to ensure they cannot be identified.

See Appendix 5, Photograph and Video Procedure, for more information on our use of photographs and videos.

14.0 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:

14.1.1 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)

14.1.2 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)

14.1.3 Integrating data protection into internal documents including this policy, any related policies and privacy notices

14.1.4 Regularly communicating with members of staff on data protection law, this policy, any related policies and any other data protection matters

14.1.5 Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

14.1.6 Appropriate safeguards being put in place if we transfer any personal data outside of UK, where different data protection laws will apply

14.1.7 Maintaining records of our processing activities, including:

i. For the benefit of data subjects, making available the 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)

ii. 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 using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure

15.0 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:

15.1.1 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

15.1.2 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

15.1.3 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

15.1.4 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

15.1.5 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)

16.0 **Disposal of Records**

The Trust regularly reviews the records held to ensure that information is disposed of in accordance with the data retention guidelines as advised in the "Information and Records Management Society's Toolkit for Schools". 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.

17.0 **17. Personal Data Breaches**

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

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

17.1.3 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:

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

18.0 **Training**

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

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

19.0 **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.

Please refer to the Freedom of Information (FOI) Policy and Publications Scheme for further information and how to make a FOI request.

20.0 **Remote Working Procedures**

20.1.1 Remote workers have the responsibility to ensure the security and safekeeping of any confidential information provided and accessed via The Trust/School. Data protection law does require organisations and individuals to ensure that personal data remains protected when being handled off site or on personal devices. Personal information should not be accessible to family or visitors

of the employee. When working remotely, all employees are bound by all the terms and conditions in their contract of employment, including terms related to confidentiality.

20.1.2 Remote working and the use of personal devices increases the security risks around personal data. The Trust/School employees remain responsible for ensuring that any personal data that is handled off site is processed in accordance with GDPR.

20.1.3 The following guidelines have been implemented by the Trust to ensure appropriate technical and organisational measures have been put into place to protect personal data:

i. Appropriate data protection training including newsletters and updates, to ensure staff understand their data protection obligations and how to reduce security risks.
ii. Devices issued by the school will be encrypted with a password (as should your personal devices – this is an ICO expectation).
iii. Staff will be able to access personal data on a secure cloud service, or a server in the IT network that's accessible through a virtual private network (VPN), so data is not stored on their devices.

20.1.4 Personal devices, unsecured Wi-Fi networks, and phishing scams, amongst others, pose potential threats and all employees are advised to implement the following to ensure compliance with the Data Protection Principles and to protect personal data:

i. Technology and devices: where provided by The Trust/School should be used over personal devices. Personal devices pose the most security risks and should only be used with an immediate need to work remotely with no other remote working capability.
ii. Encryption of portable and personal devices: personal device encryption to be enabled if staff are working from personal devices. Encryption of hard drive - this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
iii. Data should not be moved into other insecure storage: (personally-owned USB sticks and external hard drives), as this increases the potential for loss.
iv. Staff should not use insecure methods to communicate: such as personal email accounts, as this may result in compromise of personal data.
v. Awareness of the environment: care must be taken when working from home to prevent any inadvertent data breaches, for example by using laptop privacy screens; locking computers when away; and taking care when speaking on the telephone or in video conferences that virtual assistant listening devices, such as Alexa and Google Assistant, are not “listening” or “recording”.
vi. Family members and friends: should not be able to see or access any personal data held electronically or manually.
vii. Sharing: Avoid sharing the devices among family or friends.
viii. Third-party video conferencing software: If using third-party software, ensure that privacy settings are configured to protect personal data and to mitigate the risk of exploits, e.g. only the meeting host is able to share screens and files. One of the most effective security measures you can take is to keep all your software up-to-date, and video conferencing software is no exception. If you have installed a video conferencing app, keep it up to date by applying all available software updates regularly. If you access a video conferencing service via a web browser, then make sure the browser is kept up to date too.
ix. Keep the device password-protected: strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
x. Inactive device: make sure the device locks if left inactive for a period of time.
xi. Install antivirus and anti-spyware software: make sure your device is protected.
xii. Keep operating systems up to date: always install the latest updates.

xiii. Look out for phishing emails: “phishing” emails try and trick users into clicking on a bad link. Once clicked, the user is sent to a dodgy website which could download malware onto your computer, or steal passwords.
xiv. Collecting data: try to collect and share as little personal data as possible to complete your purpose.
xv. Printing: try not to print personal data unless absolutely necessary. If you are unable to use a shedder, then safely store print outs until you can take them into the school office and dispose of them securely.

21.0 **Monitoring Arrangements**

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and shared with the full governing board.

22.0 **Links with other policies and procedures -** This data protection policy is linked to our:

i. Personal Data Breach Procedure
ii. Biometric Recognition System
iii. Procedure for the Management of CCTV Photograph and Video Procedure
iv. Procedure for Dealing with a Freedom of Information Request
v. Freedom of Information Policy and Publication Scheme
vi. Safeguarding and Child Protection Policy

Appendix 1: Data Breach Response plan

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

1.1 A member of staff within the Trust who becomes aware of a suspected or actual data security breach must inform their Principal or the CEO and DPO by email immediately. The email address for contacting the DPO is dataprotection@unityschools.co.uk.

1.2 If a member of staff is unsure if a breach has happened, the above procedures must still be followed immediately so that the suspected breach can be investigated in order to establish whether a breach has happened and, if so, whether it needs to be notified to the ICO or the data subjects.

1.3 The Principal and the CEO are then responsible for assessing whether the breach or suspected breach needs to be formally escalated to the DPO. If they decide not to escalate it to the DPO, the Data Breach Log in must be completed as accurately as possible, including the reasons why the incident does not need to be escalated to the DPO. Therefore, information regarding the incident should be emailed to the DPO without delay for record keeping purposes at the email address dataprotection@unityschools.co.uk.

1.4 If the Principal or the CEO decides to escalate a breach or suspected breach to the DPO, they must do so without delay. Where possible, the report of the breach must be made by setting the information out in an email to the DPO.

1.5 Once a breach or suspected breach has been reported to the DPO, the DPO must commence an investigation and assess whether he / she has sufficient information to identify next steps. The purpose of the investigation is to:

1.5.1 Establish if a breach has happened

1.5.2 Establish the nature and cause of the breach

1.5.3 Establish the extent of the damage or harm that results or could result from the breach

1.5.4 Identify the action required to stop the data security breach from continuing or recurring

1.5.5 Mitigate any risk of harm that may continue to result from the breach

1.6 The DPO should contact the CEO if further information is required. The DPO may also need to speak to the member of staff who first reported the breach or suspected breach.

1.7 During the course of his or her investigation, the DPO should consider whether to involve the Data Breach Response Team which consists of:

Chief Executive Officer

Chair of Local Governing Council

Chair of Trustees

Head of relevant school

1.8 If the DPO is unavailable for any reason, for example, the DPO is on annual leave, on sickness absence or is otherwise not available to respond to the data breach, then The Chief Executive Officer will fulfil the responsibilities of the DPO set out in this Data Breach Response Plan. The Chief Executive Officer must have access to the email account identified above to which data breaches are reported.

1.9 If the DPO decides to involve the Data Breach Response Team, the above individuals should be copied into email correspondence and provided with regular updates on the investigation and response to the incident.

1.10 The DPO should consider whether input is required from the Trust's IT or HR team, in order to further investigate the incident, including the extent of the incident and whether any steps need to be taken to contain any breach.

1.11 Depending on the circumstances, the DPO should also consider whether the Trust should be notified in accordance with policy terms, whether legal advice is required and if the incident needs to be reported to the Police or local authority.

1.12 If the breach or suspected breach has occurred at one of our Data Processors, the DPO must liaise with the Data Processor to obtain as much information as possible about the extent of the breach or suspected breach and any steps being taken to mitigate any risk to data subjects.

1.13 The same requirement applies if the breach or suspected breach is reported to us by a joint Data Controller though in this case we need to establish with the joint Data Controller who is going to report the breach to the ICO and the data subjects if such notification is required.

1.14 Depending on the timescales as to when a member of staff originally became aware of a breach, the DPO must be mindful of the requirement to notify the ICO without delay and within 72 hours unless it is unlikely to result in a risk to the rights and freedoms of individuals. As stated above, it is therefore possible that a data security breach may need to be reported to the ICO before the school has fully investigated or contained the breach. A report to the ICO must contain the following information:

1.14.1 The nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned

1.14.2 The name and contact details of the DPO or other contact point where more information can be obtained

1.14.3 The likely consequences of the personal data breach

1.14.4 The measures taken or proposed to be taken by the school to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

1.15 The DPO is not required to provide precise details in the report to the ICO if this information is not available and an updated report can be made as and when further details come to light. Such further information may be provided in phases without undue further delay. The DPO should inform the ICO if the school does not yet have all the required information and if further details will be provided later on.

1.16 If a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred, this information could then be added to the information already given to the ICO and the incident recorded accordingly as not being a breach. There is no penalty for reporting an incident that ultimately transpires not to be a breach.

1.17 In the event that a notifiable breach is not reported to the ICO within 72 hours, a report should be made without delay with the reasons for the delay.

1.18 If the DPO concludes that a referral to the ICO is required and also concludes that there is likely to be a high risk to the rights and freedoms of individuals resulting from the data security breach then the data subjects affected by the breach must also be notified without undue delay. The DPO must liaise with The Chief Executive Officer and the Business Director and Chief Financial Officer in relation to how the issue should be communicated to the relevant stakeholders. The DPO will need to consider which is the most

appropriate way to notify affected data subjects, bearing in mind the security of the medium as well as the urgency of the situation. The notice to the affected individuals should contain the following information:

1.18.1 Description of the nature of the breach;

1.18.2 The name and contact details of the DPO or other contact point;

1.18.3 A description of the likely consequences of the breach; and

1.18.4 A description of the measures taken or proposed to be taken by the school to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

Given that a large number of our stakeholders are children, if a data breach affects our pupils, it is likely that the above information will need to be given to parents / carers. If the DPO decides to notify data subjects about a breach, the notification should at the very least include a description of how and when the breach occurred and what data was involved. Details of what the organisation has already done to respond to the risks posed by the breach should also be included. Trust should also, where appropriate, provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords in the case where their access credentials have been compromised.

1.19 The DPO must complete the Data Breach Log before making the referral to the ICO and keep it under review as and when further information comes to light.

1.20 In certain circumstances, where justified, and on the advice of law-enforcement authorities, the Trust may delay communicating the breach to the affected individuals until such time as it would not prejudice such investigations. However, data subjects would still need to be promptly informed after this time.

1.21 Even if the DPO initially decides not to communicate the breach to the affected data subjects, the ICO can require us to do so, if it considers the breach is likely to result in a high risk to individuals.

1.22 In the event that the DPO concludes that it is not necessary to refer the breach to the ICO, the DPO must still complete the Data Breach Log and clearly set out the reasons why the DPO is satisfied that a referral is not required. The DPO must keep the decision under review and be prepared to make a referral to the ICO if any circumstances change or if any information comes to light which means that a referral should be made.

1.23 Once the breach has been contained and action taken to stop or mitigate the breach, the DPO must then review the incident and identify any steps which need to be taken in order to prevent a similar breach occurring in future. This may also include whether any disciplinary action is required against any members of staff or pupils.

1.24 As part of the review process, the DPO should undertake an audit which should include a review of whether appropriate security policies and procedures were in place and if so, whether they were followed. The audit should include an assessment of any ongoing risks associated with the breach and evaluate the school's response to it and identify any improvements that can be made. The review should also consider the effectiveness of this Data Breach Response Plan and whether any amendments need to be made to it.

1.25 Where security is found not to be appropriate, the DPO should consider what action needs to be taken to raise data protection and security compliance standards and whether any staff training is required.

1.26 Where a data processor caused the breach, the DPO should consider whether adequate contractual obligations were in place to comply with the GDPR and if so, whether the data processor is in breach of contract.

2. **Sensitive Data**

Sensitive information being disclosed via email (including safeguarding records)

2.1 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

2.2 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

2.3 If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT department to recall it

2.4 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

2.5 The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request

2.6 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

2.7 If safeguarding information is comprised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

3. **School holidays**

3.1 The Trust recognises that there are times throughout the year when our ability to identify and respond to a breach swiftly and robustly may be impeded because the schools are closed during school holidays. A breach may still occur during these periods and we will implement the following steps to mitigate any risk caused if a breach happens during the school holidays:

3.1.1 Staff should contact the CEO in the first instance as opposed to the DPO, during school holidays. The DPO's email address will be made available to staff and will be available on our website and in our privacy notices so that a member of staff can be contacted should an incident occur. This email address will be monitored regularly by the assigned member of staff.

3.1.2 The CEO will have the contact details for the Principal and the DPO so that action can be taken without delay should a breach occur.

3.1.3 The CEO should follow the steps set out above as best as they can in the circumstances. In particular, this should include reporting notifiable breaches to the ICO within 72 hours and, if required, the affected individuals. The report to the ICO should state that the school is closed due to the school holidays and, depending on the circumstances, advice should be sought from the ICO on the steps the school should take to mitigate any risks.

Appendix 2: Subject Access Request Form

Please note we may be able to respond to requests more swiftly if they are made using our Subject Access Request. **Please complete a copy of the form on the following page.** Please email the DPO on dataprotection@unityschools.co.uk if you are experiencing any issues with this.

Subject Access Request (SAR) Form

Application for access to your personal data held by the Unity Schools Trust, including any schools within the Trust

Your Subject Access Rights

Subject to certain exceptions, you have a right to have access to and/or correct any personal information that the Unity Schools Trust ("the Trust") and its schools hold about you (your 'personal data').

If you wish to make a Subject Access Request, please complete this form carefully and follow the instructions regarding the provision of proof of identity and details of how to return the form to the Trust.

The purpose of this form is to ensure that all necessary information to complete your Subject Access Request is provided to the Trust. You are not obliged to use this form, but if you do not, please ensure that all necessary information on this form is provided.

The term "data subject" refers to the person about whom the information is being requested.

Section 1 – Details of the Data Subject

Title (please select one)	Mr Mrs Miss Ms Other (please state) ……
First Name	
Surname Name	
Correspondence Address	
Contact Number	
Email Address	
Information Requested	

Section 2 - Are you the Data Subject?

Yes If you are the data subject, please go to Section 4	No If you are acting on behalf of the data subject, please go to Section 3

Section 3a - Details of the Person Requesting the Information (if different to Section 1)

Title (please tick one)	Mr Mrs Miss Ms Other (please state) ……
First Name	
Surname Name	
Organisation (if applicable)	
Correspondence Address	
Contact Number	
Email Address	

Section 3b – Relationship with Data Subject

Please describe your relationship with the data subject that leads you to make this request on their behalf:

Section 4 – Authority to Release Information

A representative will need to obtain permission from the data subject before personal data can be released. The representative should obtain the data subject's signature below, or provide a separate note of authority. The representative may be asked to provide proof of identity. *If the data subject lacks capacity to give permission in this way, such as under the age of 12 or any other reason then please leave blank.* *I am the person named in Section 1/I hereby give permission for the representative named in Section 3 of this form to make a Subject Access Request (SAR) on my behalf:*

Signature of Data Subject: ……	Date: ……

Appendix 3: Biometric Recognition System

1.0 **Biometric recognition systems**

1.1 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.

1.2 <u>1) Protection of Freedom Act 2012</u>

1.2.1 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.

1.2.2 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.

1.2.3 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.

1.2.4 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.

1.2.5 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).

1.3 <u>2) Consent for the General Data Protection Regulation (GDPR) 2018 Compliance</u>

1.3.1 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.

1.3.2 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.

1.3.3 This means, for example, we will:

i. Store biometric data securely to prevent any unauthorised or unlawful use.

ii. 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.

iii. Ensure that biometric data is used only for the purposes for which they are obtained and that such data is 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 Information Policies, available to download from our trust website.

2.0 **Declaration – Biometrics Recognition Systems**

Consent is obtained using Edulink and written back to the school's MIS.

i. I have received and read the Biometrics recognition systems information provided by the school.
ii. 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.
iii. 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.
iv. 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.
v. I understand that when the student leaves the school their biometric data will be securely deleted.
vi. 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".

Appendix 4: Procedure for the Management of CCTV

1.0 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 CCTV system is owned and operated by the Trust, the deployment of which is determined by the Head of IT and Network Services and Principal in each school.
1.4 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.
1.5 The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and members of the school community.
1.6 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.
1.7 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.

2.0 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 endeavored 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.

3.0 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.

4.0 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:

i. 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 Principal 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.

5.0 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.

6.0 Enquiries

Enquiries about the operation of CCTV within our schools should be directed to the Chief Technology Officer, at cto@unityschools.co.uk.

7.0 Further Information

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

i. CCTV Code of Practice Revised Edition 2017 (published by the Information Commissioners Office) Version 1.2

ii. www.ico.org.uk

iii. Regulation of Investigatory Powers Act (RIPA) 2000

8.0 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:

i. That the area is covered by CCTV surveillance and pictures are recorded

ii. The purpose of using CCTV

iii. The name of the school

iv. 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 investigated.			
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.			

1.0 **Appendix 5: 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.

1.1. 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.

1.2. 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.

1.3. If a parent/carer 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.

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

2.0 **Photographs for Internal Use**

i. 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.
ii. 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.
iii. 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.

3.0 **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.

4.0 **Media Use**

i. 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.
ii. 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.
iii. 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.
iv. 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.

4.1 **Family Photographs at Trust Events**

i. It shall be at the discretion of the Trust whether photographs may be taken at a school event.
ii. Family and friends taking photographs for the family album will not be covered by Data Protection legislation.
iii. 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 5.1

To comply with the General Data Protection Regulations 2018 **Photographic Images of Student - Consent is obtained using Edulink and written back to the school's MIS.**

Photographic Consent types :

Internal Permission – School Displays, Presentations, Events, Newsletter, Website

External Permission - Press, Newsletter, Television, Social Media