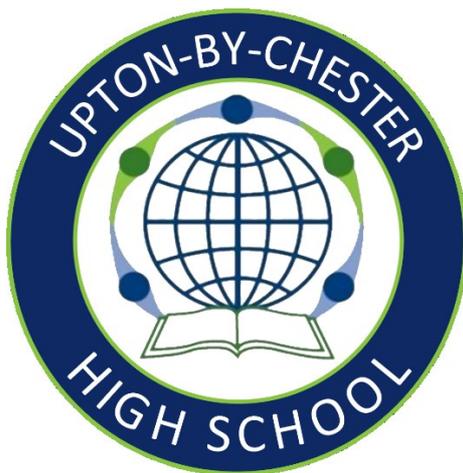


Upton-by-Chester High School

Data Protection Policy



Policy Link	
SLT	Jon Arnull

To	Date
Committee Finance and Buildings	06/10/21
Full Governing Body	08/12/21
Next Review	01/09/22

'Learning to shape the future'

Contents

1. Aims	2
2. Legislation and guidance	2
3. Definitions	3
4. The data controller	4
5. Roles and responsibilities	4
6. Data protection principles	5
7. Collecting personal data	5
8. Sharing personal data	7
9. Subject access requests and other rights of individuals	7
10. Parental requests to see the educational record	9
11. Biometric recognition systems	9
12. CCTV	9
13. Photographs and videos	10
14. Data protection by design and default	10
15. Data security and storage of records	11
16. Disposal of records	11
17. Personal data breaches	11
18. Training	12
19. Policy review frequency	12
20. Links with other policies	12
Appendix 1: Personal data breach procedure	13

1. Aims

Our school aims to ensure that all personal data collected about staff, learners, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

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:

- > UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- > [Data Protection Act 2018 \(DPA 2018\)](#)

It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#).

It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data.

It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child's educational record.

3. Definitions

TERM	DEFINITION
Personal data	<p>Any information relating to an identified, or identifiable, living individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"> > Name (including initials) > Identification number > Location data > Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> > 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	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
Data subject	<p>The identified or identifiable individual whose personal data is held or processed.</p>
Data controller	<p>A person or organisation that determines the purposes and the means of processing of personal data.</p>
Data processor	<p>A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.</p>
Personal data breach	<p>A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.</p>

4. The data controller

Our school processes personal data relating to parents, learners, staff, governors, visitors and others, and therefore is a data controller.

The school is registered with the ICO and has paid its data protection fee to the ICO, as legally required.

5. Roles and responsibilities

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

5.1 Governing body

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer (DPO)

The role of DPO to our school is carried out by an experienced and qualified member of staff designated by Cheshire West & Chester Council. The DPO operates independently, their role being to:-

- Advise our school and our employees about their obligations to comply with GDPR and other data protection requirements – this could be to assist in implementing a new CCTV system or to respond to questions or complaints about information rights.
- Monitor our school's compliance with GDPR, advising on internal data protection activities such as training for staff, the need for data protection impact assessments and conducting internal audits.
- Act as the first point of contact with the ICO and for individuals whose data our school processes.

The contact details for our appointed DPO are:

Schools Data Protection Officer

Cheshire West and Chester Council

3rd Floor

Civic Way

4 Civic Way

Ellesmere Port

CH65 0BE

Email: schoolDPO@cheshirewestandchester.gov.uk

Within school we have a nominated Data Protection Lead, whose contact details are:-

Mr J Arnull

Deputy Headteacher

Upton-by-Chester High School

St James Avenue

Chester

CH2 1NN

Email: arnullj@uptonhigh.co.uk

5.3 Headteacher

The headteacher acts 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 DP Lead 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 UK
 - 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 UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

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

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest or exercise its official authority**

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

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

- The individual (or their parent/carer when appropriate in the case of a learner) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- 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
- 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
- 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

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

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

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.

7.2 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.

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 school's record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a learner or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and learners – for example, IT companies. When doing this, we will:
 - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
 - Establish a contract with the supplier or contractor 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

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 learners or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

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 school 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual

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

If staff receive a subject access request in any form they must immediately forward it to the school's DP Lead.

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 learners at our school may not be granted without the express permission of the learner. This is not a rule and a learner's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the learner or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- 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
- 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.

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 (in certain circumstances)
- Prevent use of their personal data for direct marketing

- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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 DP Lead / DPO. If staff receive such a request, they must immediately forward it to the DP Lead.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a learner) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the learner concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the learner or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Biometric recognition systems

Where we use learners' biometric data as part of an automated biometric recognition system (i.e. learners 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](#).

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

Parents/carers and learners 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 learners. For example, learners can be issued with unique PIN codes for cashless catering purposes.

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

As required by law, if a learner 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 learner's parent(s)/carer(s).

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

12. CCTV

We use CCTV in various locations around the school site 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 accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Mr Stott (Strategic ICT Manager).

13. Photographs and videos

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

We will obtain written consent from parents/carers, or learners aged 16 and over, for photographs and videos to be taken of learners 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 learner. Where we don't need parental consent, we will clearly explain to the learner how the photograph and/or video will be used.

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

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website 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 our Safeguarding and Promoting the Welfare of Children & Young People Policy for more information on our use of photographs and videos.

14. Data protection by design and default

- 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 data protection 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
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our school 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

15. Data security and storage of records

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 held securely when not in use
- > Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- > Passwords that are at least 8 characters long containing a mixture of upper and lower case letters and numbers are used to access school computers, laptops and other electronic devices (see our ICT Acceptable Use Policy). Staff and learners are reminded that they should not reuse passwords from other sites
- > Storing any personal data on portable storage devices (e.g. USB sticks) must be protected by encryption software
- > Staff, learners 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 will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on 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 school will make all reasonable endeavours 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 72 hours after becoming aware of it. 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 learners 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 learners

18. Training

All staff and governors are provided with data protection training as part of their induction process and throughout their tenure with the school where changes to legislation, guidance or the school's processes make it necessary.

19. Policy review frequency

This policy will be reviewed annually and approved by our Governing Body.

20. Links with other policies

This data protection policy is linked to our:

- > Freedom of information publication scheme
- > ICT Acceptable Use Policy
- > Safeguarding and Promoting the Welfare of Children & Young People Policy

Appendix 1: Personal data breach procedure

1. Policy Statement

Our school holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by our school and all of our school staff, governors, volunteers and contractors, referred to herein after as 'staff'.

2. Purpose

This breach procedure sets out the course of action to be followed by all staff in our school.

3. Legal Context

Our school will comply with the requirements of Article 33 of the General Data Protection Regulation in relation to the notification of a personal data breach to the supervisory authority (ICO).

In the case of a personal data breach, the controller (the school) shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach, via the CW&C Schools DPO, to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

A processor (e.g. member of staff processing personal data on behalf of the controller (the school)), shall notify the controller without undue delay after becoming aware of a personal data breach.

The notification to the ICO referred to in paragraph 3.1 shall at least:

- > Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- > Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- > Describe the likely consequences of the personal data breach; and
- > Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The controller (the school) shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

4. Types of Breach

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of learner, staff or governing body data and/ or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment Failure
- Poor data destruction procedures
- Human Error
- Cyber-attack
- Hacking

5. Managing a Data Breach within Our School

In the event that the school identifies, or is notified of, a personal data breach, the internal procedure staff must follow is as defined below.

The person who discovers, or receives a report of, a breach must promptly notify the school's DP Lead (Mr Arnall), or the Headteacher, and complete a "School Information Security Incident Report Form" to the best of their ability, forwarding it via email to the DP Lead (or Headteacher). If the breach occurs, or is discovered, outside normal working hours, its reporting should be done as soon as is practicable, due to the short timescale permitted for the reporting of any serious breaches to the ICO.

The DP Lead (or nominated representative) will alert the Schools DPO about the reported breach and seek guidance and clarification (as applicable) as to the actions to take and whether the breach is reportable to the ICO. The DP Lead will log the data breach incident on CW&C's DPO web portal.

The DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

The DPO (or nominated representative) must inform the Head/Chair of Governors as soon as possible if the breach is considered of a serious nature. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation following a formal agreed investigation process.

The DPO (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School's legal support should be obtained.

The DPO will take the decision based on the severity of a breach and the likely effect on data subjects as to whether the ICO should be notified (this should occur within 72 hours of the incident being identified) and to whether the data subject should be notified.

The DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage.