Data Protection Policy

(including Biometric data)

Quest Learning Trust

Responsibility	Trust Board
Author	DPO
Approved date	October 2026
Next review	October 2027
Version control	V1

This document sets out the regulations for the MAT and member academies and remains in force until superseded

Contents

1. Aims 3
2. Legislation and Guidance 3
3. Definitions 3
4. The Data Controller 4
5. Roles and Responsibilities 4
5.1 The Trust Board 4
5.2 Data Protection Officer 4
5.3 Headteacher 5
5.4 All Staff 5
6. Data Protection Principles 5
7. Collecting Personal Data 5
7.1 Lawfulness, Fairness and Transparency 5
7.2 Limitation, Minimisation and Accuracy 6
7.3 Processing of special categories of personal data and criminal offence data 6
8. Sharing Personal Data 9
9. Subject Access Requests and Other Rights of Individuals 10
9.1 Subject Access Requests 10
9.2 Children and Subject Access Requests 10
9.3 Responding to Subject Access Requests 11
9.4 Other Data Protection Rights of the Individual 12
10. Parental Requests to see the Educational Record 13
11. Biometric Recognition Systems 13
12. CCTV 15
13. Photographs and Videos 15
14. Data Protection by Design and Default 16
14.1 Data Protection Impact Assessments (DPIAs) 16
15. Data Security and Storage of Records 17
16. Disposal of Records 18
17. Personal Data Breaches 18
18. Training 19
19. Monitoring Arrangements 19
Appendix 1: Personal Data Breach Procedure 20
Actions to Minimise the Impact of Data Breaches 21

1. Aims

Quest Learning Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

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 GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests. 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	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental

	• Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

Quest Learning Trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

Quest Learning Trust is registered as a data controller with the ICO (registration number ZA492928) and will renew this registration annually or as otherwise legally required.

5. Roles and Responsibilities

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

5.1 The Trust Board

The Trust Board has overall responsibility for ensuring that the trust complies with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring the Trust's compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO will provide an annual report of their activities directly to the trust board and, where relevant, report to the board their advice and recommendations on trust 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 SLA.

The DPO is SchoolPro TLC Limited and is contactable via DPO@SchoolPro.uk

5.3 Headteacher

The CFOO acts as the representative for the data controller on a day-to-day basis. This responsibility is delegated to the headteacher of each school for their function as data controllers.

5.4 All Staff

Staff are responsible for:

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

6. Data Protection Principles

The UK GDPR is based on data protection principles that the trust 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 trust aims to comply with these principles.

7. Collecting Personal Data

7.1 Lawfulness, Fairness and Transparency

Quest Learning Trust will only process personal data where the trust has one of 7 ‘lawful bases’ (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust, as a public authority, can perform a **public task,** and carry out its official functions
- The data needs to be processed so that the trust can **fulfil a contract** with the individual, or the individual has asked the trust to take specific steps before entering into a contract
- The data needs to be processed so that the trust can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed for the **legitimate interests** of the trust or a third party (provided the individual's rights and freedoms are not overridden)
- Where the above does not apply the trust shall request clear **consent** from the individual (or their parent/carer when appropriate in the case of a pupil)
- The data needs to be processed for a **recognised legitimate interest** set out in UK data protection law. These are specific, pre-approved purposes where the law has already determined that processing is lawful and proportionate, meaning the school does not need to complete a balancing test.

For further detail of which lawful basis is used for each category of data, see the relevant privacy notice.

For special categories of personal data, the trust will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018. This is laid out in more detail in point 7.3.

If the trust offer online services to pupils, such as classroom apps, it intends to rely on Public Task as a basis for processing, where this is not appropriate it will get parental consent for processing (except for online counselling and preventive services).

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

7.2 Limitation, Minimisation and Accuracy

The trust will only collect personal data for specified, explicit and legitimate reasons. The trust will explain these reasons to the individuals when it first collects their data.

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

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the trust's record retention schedule.

7.3 Processing of special categories of personal data and criminal offence data

As part of statutory functions, the trust process special category data and criminal offence data in accordance with the requirements of Articles 9 and 10 of the UK General Data Protection Regulation ('UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Special Category Data

Special category data is defined at Article 9 of the UK GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

Criminal Conviction Data

Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

Appropriate Policy Document

Some of the Schedule 1 conditions for processing special category and criminal offence data require the trust to have an Appropriate Policy Document ('APD') in place, setting out and explaining the trust's procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

This section of the Data Protection Policy document explains the processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

In addition, it provides some further information about the processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements the trust's privacy notices.

Conditions for processing special category and criminal offence data

The trust process special categories of personal data under the following UK GDPR Articles:

i. Article 9(2)(a) – explicit consent
In circumstances where the trust seek consent, it makes sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

   Examples of the trust's processing include staff dietary requirements and health information it receives from the pupils who require a reasonable adjustments to access services.

ii. Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the trust or the data subject in connection with employment, social security or social protection.
Examples of the trust's processing include staff sickness absences.

iii. Article 9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person.
An example of the processing would be using health information about a pupil or member of staff in a medical emergency.

iv. Article 9(2)(f) – for the establishment, exercise or defence of legal claims.
Examples of the trust's processing include processing relating to any employment tribunal or other litigation.

v. Article 9(2)(g) - reasons of substantial public interest.
The trust is a publicly funded body and provide a safeguarding role to young and vulnerable people. The processing of personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of the role.

Examples of the trust's processing include the information it seeks or receives as part of investigating an allegation.

vi. Article 9(2)(j) – for archiving purposes in the public interest.
The relevant purpose it relies on is Schedule 1 Part 1 paragraph 4 – archiving.

An example of the processing is the transfers the trust makes to the local authority.

The trust processes criminal offence data under Article 10 of the UK GDPR

Examples of the processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.

Processing which requires an Appropriate Policy Document

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD (see Schedule 1 paragraphs 1 and 5 of the Data Protection Act).

This section of the policy is the APD for the trust. It demonstrates that the processing of special category ('SC') and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. Retention with respect to this data is documented in the Trusts retention schedules.

Description of data processed

Quest Learning Trust processes special category data about its employees that is necessary to fulfil its obligations as an employer. This includes information about health and wellbeing, ethnicity, photographs and their membership of any union. Further information about this processing can be found in the trust's staff privacy notice.

The trust process special category data about the children in its care and other members of the community that is necessary to fulfil its obligations as a trust, and for safeguarding and care. This includes information about health and wellbeing, ethnicity, photographs and other categories of data relevant to the provision of care. Further information about this processing can be found in the trust's pupil privacy notice.

The trust also maintains a record of its processing activities in accordance with Article 30 of the UK GDPR.

Schedule 1 conditions for processing

Special category data

The trust processes special category data for the following purposes in Part 1 of Schedule 1:

- Paragraph 1(1) employment, social security and social protection.

The trust process special category data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:

- Paragraph 6(1) and (2)(a) statutory, etc. purposes
- Paragraph 18(1) – safeguarding of children and of individuals at risk

Criminal offence data

The trust processes criminal offence data for the following purposes in parts 1, 2 and 3 of Schedule 1:

- Paragraph 1 – employment, social security and social protection
- Paragraph 6(2)(a) – statutory, etc. purposes
- Paragraph 12(1) – regulatory requirements relating to unlawful acts and dishonesty etc
- Paragraph 18(1) – safeguarding of children and of individuals at risk
- Paragraph 36 – Extension of conditions in part 2 of this Schedule referring to substantial public interest

8. Sharing Personal Data

The trust will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of the staff at risk
- It needs to liaise with other agencies – it may seek consent if necessary before doing this
- The trust's suppliers or contractors need data to enable us to provide services to the staff and pupils – for example, IT and communication companies, education support companies, and those that provide tools for learning. When doing this, the trust will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data it shares
    - 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

The trust will also share personal data with law enforcement and government bodies where it is legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings

- Where the disclosure is required to satisfy safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

The trust may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any pupils or staff.

Where it transfers personal data to a country or territory outside the European Economic Area, the trust will ensure appropriate safeguards are in place, such as adequacy decisions or Standard Contractual Clauses, in accordance with 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 trust holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

It is recommended subject access requests are submitted in writing, either by letter or email to the DPO. They should include:

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

If staff receive a subject access request, they must immediately forward it to the CFOO/DPO.

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.

The ability of a child to make a request is assessed based on their competence and maturity. It is essential to determine whether the child understands their rights and the implications of the request.

In our trust, we evaluate each request on a case-by-case basis to ensure that the child's ability to understand their rights is adequately considered. Consequently, while parents or carers may generally make SARs on behalf of pupils, the child's perspective and capacity to comprehend their rights will always be considered in our decision-making process.

9.3 Responding to Subject Access Requests

When responding to requests, the trust:

- May request identification where necessary and proportionate to the request and only to the extent required to confirm an individual's identity before releasing personal data
- 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,
    - any information we request to confirm the identify of the person the information is about,
    - any information we request to confirm that a third party is authorised to act on behalf of the person, or
    - a fee (in limited, specific circumstances)
- 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
- If the request requires clarification, the time limit pauses on the day we request clarification and resumes the day after we receive it. This is referred to as 'stopping the clock'. We will not request clarification on a blanket basis, but only when reasonably required.

We will not disclose information if it:

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

When responding to a Subject Access Request, we will carry out reasonable and proportionate searches to locate personal data. This means we will:

- Identify systems and records where relevant personal data is likely to be held.
- Avoid excessive or irrelevant searches that would place an undue burden on the organisation.
- Take into account the nature of the request, the context of the data, and the effort required to retrieve it.

This approach ensures we meet our obligations while balancing practicality and fairness.

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

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

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

Requests will be processed in accordance with the Department for Education guidance Dealing with subject access requests (SARS). This guidance also makes reference to "Dealing with information already held by the requestor":

> **If a requester already has information previously provided by the school or has access to information, you do not need to resend this in your response. You will still need to explain that you hold that information and explain why you are not releasing it.** Data protection in schools - Dealing with subject access requests (SARs) - GOV.UK

The UK GDPR does not prevent a data subject making a subject access request via a third party. Requests from third parties are dealt with as follows:

- In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the data subject.
- It is the third party's responsibility to provide evidence of this entitlement.
- This might be a written authority to make the request, or it might be a more general power of attorney.
- If there is no evidence that the third party is authorised to act on behalf of the data subject, we are not required to respond to the SAR.
- However, if we are able to contact the data subject, we will respond to them directly to confirm whether they wish to make a SAR.

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 the trust is collecting their data about how it uses and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time, where consent is the basis for processing
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- You have the right to receive information about significant decisions made solely through automated means, and to seek human review, make representations and challenge those decision
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO

- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

Under Section 164A of the Data Protection Act 2018, you have a statutory right to complain if you believe your personal data has been handled inappropriately.

If you wish to raise a concern about how we process your personal data, please contact us directly at enquiries@qlt.org.uk. We will acknowledge your complaint within 30 days of receipt and take appropriate steps to investigate and respond without undue delay.

If you are not satisfied with our response, you may escalate your complaint to the Information Commission at: Information Commissioner's Office

It is important to note that the trust could be reported to the Information Commissioner's Office (ICO) for failing to comply with their statutory responsibilities regarding subject access requests and other data protection rights of the individual, and penalties (including financial) may apply.

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 records if the child attends a maintained school.

There is no equivalent legal right to access their child's educational record if the child attends an academy or free school in England or an independent school. The trust has made the decision to grant equivalent access to the parents of pupils in line with the ICO's guidance, in order to retain appropriate communication between parents and the trust.

11. Biometric Recognition Systems

11.1 What is Biometric Data?

Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

Schools that use pupils' biometric data must treat the data collected with appropriate care and must comply with the data protection principles as set out in the UK General Data Protection Regulation.

The Information Commissioner considers all biometric information to be personal data as defined by the UK General Data Protection Regulation; this means that it must be obtained, used and stored in accordance with the Regulation.

Personal data used as part of an automated biometric recognition system must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.

The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools, academies and colleges when used as part of an automated biometric recognition system.

Schools must ensure that the parent/carer of each pupil is informed of the intention to use the pupil's biometric data as part of an automated biometric recognition system. Parents/carers must be advised that alternative methods to biometric scanning are available for processing identity if required.

The written consent of the parent/carer or the pupil, where the pupil is deemed to have the capacity to consent, must be obtained before the data is taken from the pupil and processed within the biometric recognition system. In no circumstances can a pupil's biometric data be processed without written consent.

Schools and academies must not process the biometric data of a pupil where:

a) the pupil (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;

b) a parent or pupil has not consented in writing to the processing; or

c) a parent or pupil has objected in writing to such processing, even if another parent has given written consent.

Schools must provide reasonable alternative means of accessing the services to those pupils who will not be using an automated biometric recognition system.

Please also see the DfE's 'Protection of biometric data of children in schools and colleges - July 2022' for further guidance.

11.2 What Is an Automated Biometric Recognition System?

An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed above.

11.3 What Does Processing Data Mean?

'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it.

An automated biometric recognition system processes data when:

a) recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;

b) storing pupils' biometric information on a database system; or

c) using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise pupils.

11.4 Who Is Able to Give Consent?

The Data Protection Act gives pupils rights over their own data when they are considered to have adequate capacity to understand. Most pupils will reach this level of understanding at around age 13.

However, the Protection of Freedoms Act 2012, which governs the use of biometric data in schools in the UK, has different requirements. Under this Act, the consent of at least one parent is required to process the biometric data of a child under 18. If the child or any parent objects, the school cannot process the child's biometric data.

We must notify each parent of a pupil or student under the age of 18 if they wish to take and subsequently use the child's biometric data as part of an automated biometric recognition system.

As long as the child or a parent does not object, the written consent of only one parent will be required for a school or college to process the child's biometric information. A child does not have to object in writing but a parent's objection must be written.

11.5 Alternative to Biometric

The school or academy will provide an alternative to biometric scanning for any parent/pupil objecting to the processing of biometric data.

11.6 Length of Consent

The original written consent is valid until such time as it is withdrawn. However, it can be overridden, at any time either parent/carer or the pupil themselves objects to the processing (subject to the parent's/carer's objection being in writing).

When the student leaves the school or academy, their biometric data will be securely removed from the academy's biometric recognition system.

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

The trust uses CCTV in various locations around it's estate site to ensure it remains safe. It will adhere to the ICO's guidance for the use of surveillance systems including CCTV.

The trust does not need to ask individuals' permission to use CCTV, but it makes 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 the Headteacher of the school.

13. Photographs and Videos

As part of school activities, photographs and recorded images of individuals within the trust may be taken.

The trust will not seek consent from parents/carers for photographs and videos to be taken of their child for educational purposes for use in the classroom and school displays. It will process these images under the legal basis of Public Task.

The trust will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. It will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on public area notice boards and in school magazines, brochures, newsletters, etc.

- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on the school/ trust website or social media pages

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.

When using photographs and videos in this way the trust will not usually accompany them with any other personal information about the child, to ensure they cannot be identified.

14. Data Protection by Design and Default

The trust will put measures in place to show that it has integrated data protection into all of the data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments (DPIAs) 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 – see section 14.1)
- 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; it will also keep a record of attendance
- Regularly conducting reviews and audits to test the trust's privacy measures and make sure it is compliant
- Maintaining records of the processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the school and DPO and all information it is required to share about how it uses and processes their personal data (via the privacy notices)
    - For all personal data that the trust holds, maintaining an internal record of the type of data, data subject, how and why it is using the data, any third-party recipients, how and why it is storing the data, retention periods and how it is keeping the data secure.

14.1 Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) is a process to help us identify and minimise the data protection risks of a project.

The trust will do a DPIA for processing that is **likely to result in a high risk** to individuals as well as any other major project which requires the processing of personal data.

It is vital that the **DPIA is completed before processing is commenced** and kept under regular review to ensure that all risks are identified and mitigated as much as possible.

The DPIA will:

- describe the nature, scope, context, and purposes of the processing;

- assess necessity, proportionality, and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

To assess the level of risk, the trust will consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

The trust will consult the data protection officer (SchoolPro TLC Ltd) and, where appropriate, individuals and relevant experts. It may also need to consult with relevant processors.

If the trust identifies a high risk that it cannot mitigate, it will consult the ICO before starting the processing.

The trust will implement the measures it identifies from the DPIA, and integrate them into it's policies, procedures, and practice.

15. Data Security and Storage of Records

The trust will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must follow the relevant trust procedures and ensure all records and copies are returned to the trust
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils, direcotrs or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see the Acceptable Use Policy).
- Where the trust needs to share personal data with a third party, it carries out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

Historical information that relates to a trust school including alumni maybe maintained as a research resource for all interested in the history of the trust and the community it serves.

Password procedures should be followed as below:

- Password length and creation
    - Passwords used to access school computers, laptops and other electronic devices should follow the NCSC "three random words" approach. This means

creating a password from three unrelated words, resulting in a long, strong and memorable passphrase (typically).

- No mandatory regular password changes
    - Staff and pupils should not be required to change passwords at regular intervals unless there is evidence or suspicion of a security breach. The focus should be on creating a strong, unique password rather than frequent changes.
- Safe password practices
    - Passwords must not be shared with anyone.
    - Avoid using personal information (such as names, dates of birth, or common words).
    - Using a passphrase based on three random words makes passwords easier to remember and harder for attackers to guess.
- Use of password managers
    - Staff are encouraged to use a reputable password manager to securely store and manage passwords, allowing unique and strong passwords to be used for each system without the need to memorise them all.
- Additional recommendations
    - Where available, multi-factor authentication (MFA**)** should be enabled to give additional protection against unauthorised access.

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 the trust cannot or do not need to rectify or update it. This is with the exception of data that is retained in our school archive as described in section 15.

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 trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal Data Breaches

The trust will make all reasonable endeavours to ensure that there are no personal data breaches.

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

When appropriate, it will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium

- Safeguarding information being made available to an unauthorised person
- The theft of a trust laptop containing non-encrypted personal data about pupils

It is important to note that the trust could be reported to the Information Commissioner's Office (ICO) for high risk data breaches and penalties (including financial) may apply.

18. Training

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

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

19. Monitoring Arrangements

This policy will be reviewed and updated **every year** and shared with the board.

Appendix 1: Personal Data Breach Procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Headteacher of the respective trust school.
- The Headteacher will investigate the report, and liaise with the CFOO to determine whether a breach has occurred. To decide, that they will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The CFOO will seek advice from the DPO and alert the respective Chair of Governors, Chief Executive Officer and Chair of the Board of Directors where necessary.
- The Headteacher will make all reasonable efforts to contain and minimise the impact of the breach, assisted by the CFOO, DPO and relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen based on the investigation to advise the CFOO further
- The DPO in conjunction with the CFOO, will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including but not limited to:
    - Loss of control over their data
    - Discrimination
    - Identity theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

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

- The CFOO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the Breach-Log document in electronic format.
- Where the ICO must be notified, the DPO or CFOO will do this via the 'report a breach' page of the ICO website. As required, the report will set out:

    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the trust will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the they expect to have further information. The CFOO or DPO will submit the remaining information as soon as possible
- The CFOO and Headteacher will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the CFOO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The CFOO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The CFOO/DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored are in the Breach-Log document in electronic format.

- The DPO, CFOO and headteacher will review what happened and how it can be stopped from happening again. This will happen as soon as reasonably possible

Actions to Minimise the Impact of Data Breaches

An example of the actions the trust will take to mitigate the impact of a data breach are set out below, focusing especially on a breach involving particularly risky or sensitive information. The trust will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidently made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

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

Other types of breach might include:

- Details of pupil premium children being published on the school website
- Non-anonymised pupil data or staff pay information being shared with governors
- *A device containing* non-encrypted sensitive personal data about a member of the trust's community being stolen or hacked.