



DATA PROTECTION AND DATA BREACH POLICY

Statutory

Approved and Authorised for use by the Trust Board 18th July 2023

History of Policy Changes

Version	Author/Owner	Drafted	Origin of Change / Comments	Changed by
1	Sarah Gibbon	May 2021	Merger of previous Data Protection Policy and Data Breach Policy	Sarah Gibbon
2	Sarah Gibbon	June 2022	Annual Review Addition/amendment to Sections 5, 6, 7, 8, 10 and 12	Sarah Gibbon
3	Sarah Gibbon	April 2023	Re-write of policy from One West recommendations	Sarah Gibbon

This policy applies to The Priory Learning Trust (TPLT) and all its academies

Date policy adopted	September 2023
Review cycle	Biannually
Review date	September 2025

Contents

1. Aims
2. Scope
3. Distribution
4. Definitions
5. Roles and Responsibilities
6. Data Protection Officer
7. Data Subject Rights
8. Data Protection Principles
9. Processing Personal Data
10. Third Parties with Access to Personal Data
11. Data Protection by Design and Default
12. Personal data breaches or near misses
13. Biometric Recognition Systems
14. Destruction of records
15. Training
16. Review and Monitoring Arrangements
17. Complaints
18. Legislation and Guidance
19. Links with Other Policies

- Appendix 1 Examples of Special Category Data that we process
- Appendix 2 Subject Access Request Procedures
- Appendix 3 Data Breach Form
- Appendix 4 Security Incident Management (SIM): Record of Work
- Appendix 5 Seven Golden Rules to Information Sharing

1. Aims

The Trustees of The Priory Learning Trust (TPLT) are committed to ensuring that all personal data collected is processed in accordance with all relevant data protection laws including the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

TPLT are registered as a data controller with the Information Commissioner.

The details of TPLT's Data Protection Officer can be found at paragraph 6.

2. Scope

This policy applies to anyone who has access to data and/or is a user of school ICT systems, both in and out of the school, including staff, governors, students, volunteers, parents / carers, visitors, contractors, and other community users.

This policy is also intended to serve as the appropriate policy document for the processing of Special Category Data and Criminal Record Data (where applicable).

This policy applies to all personal data for which the school is the Data Controller, regardless of whether it is in paper or electronic format.

Where "TPLT" or "the Trust" is used in this document, it applies to all parts of The Priory Learning Trust and its academies.

3. Distribution

This policy is available on TPLT's website and in hard copy from the school office on request.

4. Definitions

Personal data - Any combination of data items which could identify a living person and provide specific information about them, their families or circumstances. The term covers both facts and opinions about an individual. The Trust may process a wide range of personal data of staff (including governors and volunteers) students, their parents or guardians as part of its operation. A non-exhaustive list of examples of the types of personal data that we process may be found in our Privacy Notices.

Special category personal data - Formerly known as "sensitive personal data", Special Category Data is information that might not necessarily identify a person, but is a lot more sensitive to that person. These are:

- racial or ethnic origin
- political opinions
- religious / philosophical beliefs
- trade union membership
- genetic data
- biometric data (for identification purposes)
- health data (mental and physical)
- sex life or sexual orientation

Our Record of Processing Activities (RoPA) details the types of information we hold and the grounds upon which we process it, as does our Privacy Notice which can be found on our website. Examples of the types of special category data we hold may be found at Appendix 1.

Data Subject(s) - The Data Subject is the person about whom the personal data relates or identifies.

Data Processing - Data Processing is an over-arching term that means "doing something" with personal data. This commonly includes:

- Collecting or collating the data
- Analysing the data
- Sharing the data
- Storing the data
- Destroying the data

Data Controller - The Data Controller is occasionally the person or more commonly the organisation with overall responsibility for the processing of personal data that organisation undertakes. They will make all the decisions about what is captured, how it's used and the purpose for it, as well as deciding what controls need to be in place.

Data Processor - is occasionally a person, but more commonly an organisation commissioned by a Data Controller to carry out their data processing on behalf of the Data Controller. These are usually software providers such as Microsoft, or contracted out services such as an insurance company. Essentially, a Data Processor is acting as an extension of the Data Controller, so must operate under the Data Controller's instructions, and under the terms of a Data Processing Agreement.

Data Sharing - means *giving* it to another Data Controller, for them to use for their own purposes. Once you have shared personal data, the recipient becomes the Data Controller for that information, and therefore makes the decisions over what they will do with it.

Note, we do NOT *share* data with our Data Processors, as these are processing it under our Data Controllorship.

Data Breach - The most common type of data breach is the accidental or unlawful *loss, alteration, destruction, disclosure of or access to* personal data, for example sending an email to the wrong recipient, losing a file containing personal data, or sharing passwords enabling someone else to access your account. However, we consider any failing of one of the Data Protection Principles (Article 5 of GDPR) as a GDPR breach, so could include examples such as not having the necessary paperwork in place, not providing the data subject with clear privacy information, retaining personal data for longer than is necessary or processing personal data without an identified lawful basis (Article 6 of GDPR).

Data Processing Agreement – a legally binding contract between the Data Controller and its Data Processor. This contract defines exactly how the Data Controller expects the Data Processor to process its personal data, and follow standard contract clauses.


Data Sharing Agreement - a non-legally binding written agreement between Data Controllers where there is regular sharing of personal data. The Sharing Agreement should define who is involved in the agreement, what data is being shared, why the recipient needs the data, how this is lawful, the how the data will be shared.

5. Roles and Responsibilities

Data Protection is the responsibility of all staff within TPLT. The **Trustees** have overall responsibility for ensuring that our schools comply with all relevant data protection obligations.

The **Chief Executive Officer** (CEO) acts with the delegated authority of the Trustees on a day to day basis at Trust level. Each school's Principal acts with the delegated authority of the CEO on a day to day basis at school level.

All other staff (as defined in scope) - All staff are responsible for:

- Familiarising themselves with and complying with this and related policies. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes. However, staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken;
- Taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times. All staff should adopt the approach that they should treat the personal data of others with the same care with which they would treat their own;
- Only using computers and other devices authorised by the school for accessing and processing personal data ensuring that they are properly "logged-off" at the end of any session in which they are using personal data; and locking devices when they are temporarily left unattended at any point (Windows Button  + L is a handy shortcut);
- Storing, transporting and transferring data using encryption and secure password protected devices;
- Not transferring personal data offsite or to personal devices other than in accordance with the school's Bring Your Own Device policy;
- Deleting any data they hold in line with this policy, and the retention schedule;
- Informing the school of any changes to their personal data, such as a change of address;

- Reporting to the CEO or Principal, or in their absence the DPO in the following circumstances:
 - o Any questions about the operation of this policy, data protection law, retaining or sharing personal data or keeping personal data secure;
 - o If they have any concerns that this policy is not being followed;
 - o If they are unsure whether they have a lawful basis upon which to use personal data in a particular way;
 - o If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the UK and European Economic Area;
 - o The discovery of a data breach or near miss (immediate action is required) – please refer to the Data Breach Policy and section 12 of this policy;
 - o Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
 - o If they are to share personal data with a data processor, for example a contractor or someone offering a service, in which case a contract is likely to be required and potentially a data protection impact assessment, please see - *Sharing Personal Data* (section 10).

6. Data Protection Officer

The Data Protection Officer (DPO) is responsible for advising on the implementation of this policy, monitoring compliance with data protection law, providing support and developing related policies and guidelines where applicable, in amongst other data protection related functions. They will provide an annual report on compliance to the Trust and its school and, where requested, to the Trustees and, where relevant, provide TPLT with advice and recommendations on data protection issues.

The Trust has appointed One West as its DPO, and they can be contacted by email at:

One West (Bath and North East Somerset
Council)
Guildhall
High Street
Bath
BA1 5AW

Email: One_west@bathnes.gov.uk
Telephone: 01225 395959

Under usual circumstances the internal data protection lead, the Academy Operations Manager (AOM) or the Chief Analytics Officer (CAO) will be the point of contact with the DPO.

7. Data Subject Rights

In all aspects of its work, the Trust will ensure that the rights of the data subject are protected by all practicable measures associated with the conduct of the Trust's work. Subject to exceptions, the rights of the data subject as defined in law are:

1. *The Right to be informed.*

TPLT advises individuals how it will use their data through the use of transparent Privacy Notices and other documentation, such as data capture and consent forms where appropriate.

2. *The Right of access*

An individual when making a subject access request (SAR) is entitled to the following;

- Confirmation that their data is being processed;
- Access to their personal data;
- Other supplementary information – this largely corresponds to the information that should be provided in a Privacy Notice.

TPLT must respond to such a request within one calendar month unless the request is complex, in which case it may be extended by a further 2 calendar months. Please refer to Appendix 2 for further details as to how to manage a subject access request.

3. *The Right to rectification*

Individuals have the right to ask us to rectify information that they think is inaccurate or incomplete. The Trust has a duty to investigate any such claims and rectify the information where appropriate within one calendar month, unless an extension of up to a further 2 calendar months can be justified.

4. *The Right to erasure*

Individuals have a right to request that their personal information is erased but this is not an absolute right. It applies in circumstances including where:

- The information was given voluntarily, consent is now withdrawn and no other legal basis for retaining the information applies;
- The information is no longer required by the school;
- The data was collected from a child for an online service; or
- TPLT has processed the data on the basis that it is in their legitimate business interests to do so, and having conducted a legitimate interests test, it concludes that the rights of the individual to have the data erased outweigh those of the school to continue to process it.

TPLT will consider such requests as soon as possible and within one month, unless it is necessary to extend that timeframe for a further two months on the basis of the complexity of the request or a number of requests have been received from the individual.

5. *The Right to restrict processing*

This is not an absolute right. An individual may ask the Trust to temporarily limit the use of their data (for example, storing it but not using it) when it is considering:

- A challenge made to the accuracy of their data, or
- An objection to the use of their data.

An individual may also ask the Trust to restrict the destruction of a record, if they wish it to be retained beyond the normal retention period.

In addition, the Trust may be asked to limit the use of data rather than delete it:

- If the individual does not want the Trust to delete the data but does not wish it to continue to use it;
- In the event that the data was processed without a lawful basis;
- To create, exercise or defend legal claims.

6. *The Right to data portability*

An individual can make a request in relation to data which is held electronically for it to be transferred to another organisation or to themselves where they have provided it either directly or through monitoring activities e.g. apps. The Trust only has to provide the information where it is electronically feasible.

7. *The Right to object*

Individuals have a right to object in relation to the processing of data in respect of:

- a task carried out in the public interest except where personal data is processed for historical research purposes or statistical purposes
- a task carried out for the exercise of official authority
- a task carried out in its legitimate interests
- scientific or historical research, or statistical purposes, or
- direct marketing.

Only the right to object to direct marketing is absolute, other objections will be assessed in accordance with data protection principles. The Trust will advise of any decision to refuse such a request within one month, together with reasons and details of how to complain and seek redress.

8. *Rights related to automated decision making*

This does not apply as TPLT school does not employ automated decision-making processes.

8. Data Protection Principles

Data protection legislation is based on seven key data protection principles that TPLT complies with.

The principles say that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** – TPLT will explain to individuals why the Trust needs their data and why it is processing it – for example on consent forms (where consent is used as the basis for processing), and in its Privacy Notice(s). TPLT reviews its documentation and the basis for processing data on a regular basis
- **Collected for specified, explicit and legitimate purposes** – TPLT explains these reasons to the individuals concerned when it first collects their data. If the Trust wishes to use personal data for reasons other than those given when the data was first obtained, it will inform the individuals concerned before doing so, and will seek consent where necessary and appropriate unless the new purpose is compatible with that in respect of which consent was given, or there is another lawful basis for sharing the information. The Trust will document the basis for processing.
- **Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed** - TPLT must only process the minimum amount of personal data that is necessary in order to undertake its work.
- **Accurate and, where necessary, kept up to date** – TPLT will check the details of individuals on its databases at appropriate intervals and maintain the databases. It will consider and respond to requests for inaccurate data to be rectified in accordance with the Data Protection Act 2018.
- **Kept for no longer than is necessary for the purposes for which it is processed** – We review what data we hold at appropriate intervals – for example upon the annual review of the Record of Processing Activities (or sooner if needed). When TPLT no longer needs the personal data it holds, it will ensure that it is deleted or anonymised in accordance with the retention schedule. We only keep personal data, include special category data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where there is a legal obligation to do so;
 - We have a retention and disposal/records management policy which governs how long all data including special category data shall be retained for. This policy is complied with and reviewed regularly;
 - Once the data is no longer needed, we delete it, securely destroy it in line with our retention and disposal policy, or render it permanently anonymous.
- **Processed in a way that ensures it is appropriately secure** – TPLT implements appropriate technical measures to ensure the security of data and systems for staff and all users. Please refer to the Information Security Policy, IT Acceptable Use Policy, Mobile Device Policy, Password Policy and Social Media Policy, and how data is securely transferred in and out of the Trust's system.
 - We adopt a risk- based approach to taking data offsite. Unless absolutely necessary, hard copies of special category personal data will not be removed from any of our premises.
 - Any decision to remove the information must be based on the business need of the organisation or in the best interests of the individual, rather than for the convenience of the individual member of staff. It is always preferable for any special category personal data to be accessed via an appropriately encrypted means rather than via hard copy, when off-site.
 - If there is no reasonable alternative to removing hard copies from the organisation name's site, the following procedure will apply:
 - i. A record of what information has been removed will be logged on site with the office so that there is a record of what has been removed – for example health data in trip packs;
 - ii. Information will be transported and stored in a lockable case;
 - iii. Wherever possible, information that is removed from site will be pseudonymised by using a "key" held by the office on site;
 - iv. We adopt a risk- based approach, for example hard copy personal data with lower sensitivity (e.g. exercise books) may be taken off site, but if left in a vehicle must be locked in the boot, never left in a visible place, only for the shortest period of time and never overnight. Special Category Data (e.g. SEND, Safeguarding, Health data) must be kept on the staff member's person at all times.
 - v. Special category data must be returned to the Trust's premises at the end of the working day, if not on a residential school trip. If this is not practicable, and a staff

member needs to retain the information in their personal possession, this must be discussed in advance with a member of SLT including what measures will be taken to safeguard the information, given the risks that are beyond a staff member's control in so doing and the potential consequences ensuing. The relevant member of the SLT must record their decision.

- vi. Data will be tidied away when not in use (e.g. when staff undertake marking at home, it must be out of sight of family members, not left out and tidied away afterwards).
- vii. Only those who have need to access the data concerned will be granted permission and access to it.
- viii. Our data security policy / acceptable use / remote working policies describe the requirements around bring your own device, remote working and password protection

- o **Accountability** – TPLT complies with its obligations under data protection laws including the GDPR and can demonstrate this via the measures set out in this policy including completing Data Protection Impact Assessments (DPIAs) where necessary; integrating data protection into internal documents including this policy, any related policies and Privacy Notices; regularly training members of staff on all relevant data protection law, including this and any related policies; reviewing and auditing privacy measures and compliance; maintaining and reviewing records of its processing activities for all personal data that it holds; reviewing and ensuring familiarity of policies related to the handling of data; reviewing reasons for data breaches; and ensuring stakeholders manage risks and compliance using the annual compliance statement and / or Risk Register.

9. Processing Personal Data

In order to ensure that the Trust's processing of personal data is lawful, it will always identify one of the following six grounds for processing **before** starting the processing:

- The individual (or their parent/carer when appropriate in the case of a pupil/ student) has freely given clear consent. The Trust will seek consent (where appropriate) to process data from the pupil / student or parent depending on their age and capacity to understand what is being asked for.
- 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, i.e. to protect someone's life;
- The data needs to be processed so that the Trust, as a public authority, can **perform a task in the public interest, or carry out its official functions**;
- The data needs to be processed for the **legitimate interests** of the Trust or a third party where necessary, balancing the rights of freedoms of the individual. However, where the Trust can use the public task basis for processing, it will do so rather than rely on legitimate interests as the basis for processing.

9.1 Processing Special Categories of Personal Data

In addition to the legal basis to process personal data, special categories of personal data also require an additional condition for processing under Article 9 of the GDPR. The grounds that we may rely on include:

- a) The individual has given **explicit consent** to the processing of those special categories of personal data for one or more specified purposes;
- b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights under **employment and social security and social protection law and research**; a full list can be found in Schedule 1 Part 1 of the Data Protection Act 2018.
- c) Processing is necessary to protect the **vital interests** of the individual or of another natural person where the individual is physically or legally incapable of giving consent;
- d) Processing is carried out in the course of its legitimate activities by a not-for-profit organisation with a political, philosophical, religious, or trade union aim on the condition that the processing relates solely to its members, or former member who have regular contact with it, and that the personal data are not disclosed outside that body without consent.
- e) Processing relates to personal data which are **manifestly made public** by the individual;

Processing is necessary for the **establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity;

- f) Processing is necessary for reasons of **substantial public interest** but must be clearly demonstrated and assessed as part of the public interest test and evidenced throughout the decision-making process.

These grounds include the following (the full list of defined purposes may be found in Schedule 1 Part 2 of the Data Protection Act 2018):

- Statutory and government purposes
 - Safeguarding of children or individuals at risk
 - Legal claims
 - Equality of opportunity or treatment
 - Counselling
 - Occupational pensions
- g) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- h) Processing is necessary for reasons of **public interest in the area of public health**;
- i) Processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**.

Deciding upon the correct legal basis for processing data can be difficult and more than one ground may be applicable. We consult with the Data Protection Officer where appropriate.

We must also comply with Schedule 1 of the Data Protection Act (as well as Articles 6 and Article 9), when we are processing data where the conditions relate to employment, health and research or substantial public interest.

9.2 Legal basis for processing criminal offence data

Criminal offence data includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions.

We do not maintain a register of criminal convictions.

When processing this type of data, we are most likely to rely on one of the following bases:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the individual in connection with employment, social security or social protection;
- The processing is necessary for the purposes of protecting the physical, mental or emotional well-being of an individual;
- The processing is necessary for statutory purposes; or
- Consent – where freely given. The school acknowledges because of the potential for the imbalance of power that it may be difficult for consent to be deemed valid and will only rely on this where no other grounds apply.

10. Third Parties with Access to Personal Data

Please refer to the Trust's Privacy Notice(s) for details of who, aside from the Trust, has access to the personal data processed.

• Data Sharing

The Trust will only share personal data under limited circumstances, when there is a lawful basis to do so and where identified in the Privacy Notice(s). The following principles apply:

- o The Trust will share data if there is an issue with a student /pupil or third party, for example, parent/carer that puts the safety of staff or others at risk;
- o The Trust will share data where there is a need to liaise with other agencies. It will seek consent as necessary and appropriate before doing so. However, where child protection

and safeguarding concerns apply, it will apply the “Seven golden rules of information sharing.” In limited circumstances, data may be shared with external agencies without the knowledge or consent of the parent or student in line with the DPA 2018, which includes ‘safeguarding of children and individuals at risk’ as a condition that allows practitioners to share information without consent;

The Trust may also disclose personal data to law enforcement and government bodies where there is a lawful requirement / basis for us to do so, including:

- o For the prevention or detection of crime and/or fraud;
- o For the apprehension or prosecution of offenders;
- o For the assessment or collection of tax owed to HMRC;
- o In connection with legal proceedings;
- o For research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided or it is otherwise fair and lawful to do so.

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

• **Third-Party Processors**

The Trust’s suppliers and contractors including its Data Protection Officer may need data to provide services. When third parties are processing personal data on behalf of the school, the Trust will:

- o Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law;
- o Establish a data processing contract 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 where there is regular sharing;
- o Only provide access to data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the Trust.

11. Data Protection by Design and Default

The Trust has a legal obligation to integrate appropriate technical and organisational measures into all of its processing activities, and to consider this aspect before embarking on any new type of processing activity. It is a statutory requirement that any activity involving a high risk to the data protection rights of the individual when processing personal data be assessed by the Data Protection Impact Assessment. Prior to the assumption of any such activity, One West must be consulted and an initial screening be conducted assessing risk.

Please refer to the Information Security Policy for further detail as to how the school implements this principle in practice.

12. Personal data breaches or near misses

A personal data breach is defined as “*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service.*” It may be deliberate or accidental.

Wherever it is believed that a security incident has occurred, or a “near-miss” has occurred, the staff member must inform the Headteacher and DPO **immediately** in order that an assessment can be made as to whether the ICO should be informed within 72 hours as is legally required, and / or those data subjects affected by the breach. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes.

Appropriate measures are implemented to protect personal data from incidents (either deliberately or accidentally) to avoid a data protection breach that could compromise security.

This policy applies to all employees of TPLT including contract, agency and temporary staff, volunteers and employees of partner organisations working for TPLT. For the purposes of this policy data breaches will include both suspected and confirmed incidents.

An incident can include, but is not limited to:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (*e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge*)
- Equipment failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data (*e.g. login details, emails to the wrong recipient, not using BCC, post to the wrong address*)
- Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire or flood
- Human error
- Breaches of policy such as
 - o Server Room door left open
 - o Filing cabinets left unlocked
 - o Temporary loss / misplacement of confidential or sensitive data or equipment on which such data is stored (*e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge*)

Near misses can include, but are not limited to, scenarios such as emails sent to the wrong recipient where a non-delivery report bounces back.

The quick response to a suspected or actual data breach is key. All consumers in scope of this policy have a responsibility to report a suspected or actual data breach. If this is discovered or occurs out of hours then this should be reported as soon as practically possible. This should be done through the completion of the reporting form in Appendix 3, which is sent to the individual school's Business Manager who will liaise with its DPO. A separate form, "TPLT Data Breach Reporting Form" is available to aid communication.

The Lead Officer shall complete the following phases of SIM (which are detailed in Appendix 4) with advice from its Data Protection Officer:

- a) **Preparation** – the organisation will understand its environment and be able to access the necessary resources in times of incidents. It will also ensure its staff are aware of how to identify and report breaches
- b) **Identification** – the organisation will determine whether there has been a breach, or a near miss, it will also assess the scope of the breach, and the sensitivity on a risk basis.
- c) **Containment & Eradication** – the organisation will take immediate appropriate steps to minimise the effect of the breach. It will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause, and will establish who may need to be notified as part of the initial containment and will inform the police and other enforcement bodies where appropriate.
- d) **Recovery** – the organisation will determine the suitable course of action to be taken to ensure a resolution to the incident. This may include re-establishing systems to normal operations, possibly via reinstall or restore from backup.
- e) **Wrap Up / Learning from Experience (LfE)** – an assessment will be made on the likely distress on any affected data subjects. This will then form the decision on whether to report this to the regulator (ICO) which must be reported within 72 hours, and to the affected data subjects which must be done without undue delay. The organisation's Communications / Press Team may also be notified to handle any queries and release statements.

A review of existing controls will be undertaken to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring. The review will consider:

- Whether controls are sufficient
- Whether training and awareness can be amended and/or improved
- Where and how personal data is held and where and how it is stored
- Where the biggest risks are apparent and any additional mitigations
- Whether methods of transmission are secure
- Whether any data sharing is necessary

If necessary a report recommending any changes to systems, policies and procedures will be considered by the senior management board. This will include the decision on whether to report to the regulator and affected data subjects.

Phases (b) to (e) will form part of the investigation process. This process should commence immediately and wherever possible within 24 hours of the breach being discovered or reported.

13. Biometric Recognition Systems

Biometric data consists of personal information about an individual's physical or behavioural characteristics which may be used to identify that person. It may take the form of fingerprint, voice, or facial recognition. We use biometric in the follow ways:

- Cashless payment system for school meals

We will undertake a Data Protection Impact Assessment before implementing any new biometric system to assess the impact on individuals.

In accordance with the Protection of Freedoms Act 2012, once satisfied, we will notify all those with parental responsibility in the case of any student under 18, unless this is impractical (for example the whereabouts of the parent is unknown or if there is a safeguarding issue) and may only proceed if we have at least one positive written consent, and no written parental objection. We will not proceed to process the information if the student themselves objects. Either parents or the student may withdraw their consent at any time, although parents must object in writing.

In the case of adults, for example staff members, we will seek their consent direct from them before processing any biometric data.

If the individual concerned does not agree to proceed or wishes to withdraw their consent to the use of the biometric system, we will provide an alternative means of achieving the same aim.

14. Destruction of records

The Trust adheres to its retention policy and will permanently securely destroy both paper and electronic records securely in accordance with these timeframes.

The Trust will ensure that any third party who is employed to perform this function has the necessary accreditations and safeguards.

Where the Trust deletes electronic records and its intention is to put them beyond use, even though it may be technically possible to retrieve them, it will follow the Information Commissioner's Code of Practice on deleting data and this information will not be made available on receipt of a subject access request.

15. Training

To meet its obligations under Data Protection legislation, the Trust will ensure that all staff, volunteers, Trustees and Governors receive an appropriate level of data protection training as part of their induction. Permanent members of staff will receive Data Protection training at least every 12 months. Those who have a need for additional training will be provided with it, for example relating to use of systems or CCTV.

Data protection also forms part of continuing professional development. Staff members undertake regular informal discussions on Data Protection, to ensure key updates are provided where changes to legislation,

guidance or the Trust's processes make it necessary. This will include lessons learned from Data Breaches and Near Misses, preventative measures to avoid them, and other best practice as advised.

Regular information emails will be sent to all staff to raise awareness of GDPR and Cyber-security issues and remind them of key processes.

16. Review and Monitoring Arrangements

Whilst the DPO is responsible for advising on the implementation of this policy and monitoring the Trust's overall compliance with data protection law, the Trust is responsible for the day to day implementation of the policy and for making the data protection officer aware of relevant issues which may affect the Trust's ability to comply with this policy and the legislation.

This policy is reviewed annually by the Trust and where materially amended is consulted on, where necessary. We will monitor the application and outcomes of this policy to ensure it is working effectively.

Compliance with this policy shall be monitored through a review process. This will be agreed with the Data Protection Officer, and compliance will be reported to the senior management board.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the organisation, in consultation with senior management, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

Review this Policy upon; Change of Data Protection Officer, Change of Legislation

17. Complaints

The Trust is always seeking to implement best practice and strives for the highest standards. The Trust operates an "open door" policy to discuss any concerns about the implementation of this policy or related issues. The Trust's complaints policy may be found on its website.

There is a right to make a complaint to the Information Commissioner's Office (ICO), but under most circumstances the ICO would encourage the complainant to raise the issues in the first instance with the Trust or via the Trust's DPO.

The ICO is contactable at:

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113

18. Legislation and Guidance

This policy takes into account the following:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act (DPA) 2018.
- The Protection of Freedoms Act 2012
- Guidance published by the Information Commissioner's Office
- Protection of biometric information of children in schools and colleges – DfE March 2018
- Information Sharing – Advice for Practitioners – DfE July 2018.

19. Links with Other Policies

This Data Protection Policy is linked to the following:

- Information Security Policy

- Retention & Disposal / Records Management Policy
- Mobile device Policy
- Privacy Notices
- Safeguarding Policy
- IT Acceptable Use Policies
- Social Media Policy
- Password Policy
- Consent / Permissions Form
- Admissions Form

20. Review

This policy is reviewed annually by the Trust and where materially amended is consulted on, where necessary. We will monitor the application and outcomes of this policy to ensure it is working effectively.

Compliance with this policy shall be monitored through a review process. This will be agreed with the Data Protection Officer, and compliance will be reported to the senior management board.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the organisation, in consultation with senior management, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

Review this Policy upon;
Change of Data Protection Officer,
Change of Legislation

Appendix 1 – Examples of Special Category Data that we process

Examples of where we may process special category data include in@

Pupil health data and information concerning their racial/ethnic origin in admissions records and in pupil records/trip packs

Special Educational Needs information

School census information

Attendance records

Biometric data ie. Fingerprints for cashless catering

Information contained within child protection and safeguarding records

Staff applications forms

HR files including disciplinary and capability proceedings which may include DBS and right to work checks, health and equal opportunities data (disability, race, ethnicity, sexual orientation)

Accident reporting documentations

Our Record of Processing Activities (RoPA) details the types of information we hold and the grounds upon which we process it, as do our Privacy Notices which may be found on the TPLT website.

Appendix 2 - Subject Access Request Procedures

The organisation shall complete the following steps when processing a request for personal data (Subject Access Request or SAR) with advice from the DPO.

1. Ascertain whether the requester has a right to access the information and capacity.
2. Obtain proof of identity (once this step has been completed the clock can start)
3. Engage with the requester if the request is too broad or needs clarifying
4. Make a judgement on whether the request is complex and therefore can be extended to a 2 month response time
5. Acknowledge the requester providing them with
 - a. the response time – 1 month (as standard), 2 months if complex; and
 - b. details of any costs – Free for standard requests, or you can charge if the request is manifestly unfounded or excessive, or further copies of the same information is required, the fee must be in line with the administrative cost
6. Use its Record of Processing Activities and/or data map to identify data sources and where they are held
7. Collect the data (the organisation may use its IT support to pull together data sources – for access to emails the organisation can do so as long as it has told staff it will do so in its policies)
8. If (6) identifies third parties who process it, then engage with them to release the data to TPLT.
9. Review the identified data for exemptions and redactions in line with the ICO's Code of Practice on Subject Access and in consultation with the organisation's Data Protection Officer (One-West).
10. Create the final bundle and check to ensure all redactions have been applied
11. Submit the final bundle to the requester in a secure manner and in the format they have requested.

Appendix 3: Data Incident Reporting Form

(available as a separate document, "TPLT Data Breach Reporting Form" to aid communication)

1. About the incident	
Date and time of incident	
Where did the incident occur?	
Date (and time where possible) of notification to the organisation	If there was any delay in reporting the incident, please explain why this was
Who notified us of the incident?	
Describe the incident in as much detail as possible, including dates, what happened, when, how and why?	Include names of staff and data subject(s). Identifying information will be anonymised for any reporting purposes.
2. Recovery of the data	
What have you done to contain the incident?	eg limiting the initial damage, notifying the police of theft, providing support to affected data subjects
Please provide details of how you have recovered or attempted to recover the data, and when	Consider collecting the lost data, rather than relying on an unintended recipient to dispose of it
3. About the affected people (the data subjects)	
How many individuals' data has been disclosed?	
Are the affected individuals aware of the incident, and if so, what was their reaction?	
When and how were they made aware / informed?	
Have any of the affected individuals made a complaint about the incident?	
Are there any potential consequences and / or adverse effects on the individuals? What steps have been taken / planned to mitigate the effect?	

Your name and contact details:	
---------------------------------------	--

Appendix 4: Security Incident Management (SIM): Record of work

This document provides the documented evidence and audit trail of a reported information security incident. It is designed to operate alongside the organisation's Data Protection Policy, and Data Breach Policy.

This form is to be completed by the Incident Handler(s) in the organisation.

The incident may require additional input and support from the organisation's Data Protection Officer, ICT, and potentially other specialist bodies (e.g. National Cyber Security Centre – NCSC)

Incident No:	
Severity (H, M, L):	
Basis for initial severity rating:	
Incident Handler(s):	
Date reported to organisation:	
By whom:	
Date reported to Incident handler:	
By whom:	
Date incident occurred:	
Senior Management notified (date):	

Summary of breach:	
--------------------	--

Incident Response Phase	Evidence/Actions Taken
1. Preparation Gather and learn the necessary tools, become familiar with your environment	<ul style="list-style-type: none">• Necessary staff trained on incident handling and incident response• Policy, Procedures & Guidance (link to org policies)• Network Diagrams are held by ICT• The Record of Processing Activities (RoPA) will provide details of data, owners, custodians, and third parties – link to the RoPA• ICT also record event logs and hold logs on other systems (e.g. emails, firewalls etc)• INSERT ANY OTHER TOOLS WHICH WILL HELP YOU IN INCIDENT RESPONSE• Key contacts:<ul style="list-style-type: none">◦ INSERT KEY CONTACTs
2. Identification Detect the incident – Is it an incident (breach of policy), a near miss, or a data breach?	

Determine its scope, and involve the appropriate parties	
3. Containment Contain the incident to minimize its effect on other IT resources	
4. Eradication Eliminate the affected elements e.g. remove the malware and scan for anything remaining	
5. Recovery Restore the system to normal operations, possibly via reinstall or backup.	
6. Wrap Up Document the lessons learned and actions to reduce the risk of the incident/breach/near miss re-occurring Document the decision to report to both the affected data subjects and the ICO.	
	<p><i>If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay</i></p> <p>Decision to report to Data subjects - Yes / No</p> <p>Based on:</p> <p>Officer:</p> <p>Signed: _____ Date: _____</p>
	<p><i>Establish the likelihood and severity of the resulting risk to people's rights and freedoms - A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other</i></p>

	<i>significant economic or social disadvantage to the natural person concerned</i>
	Decision to report to ICO - Yes / No
	Based on:
	Officer:
	Signed: Date:

Appendix 5: Seven Golden Rules to Information Sharing

The following 'golden rules' have been taken directly from the following government guidance;

"Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers" HM Government, July 2018

The seven golden rules for sharing information

- Remember that the General Data Protection Regulations (GDPR), Data Protection Act 1998 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.
- Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
- Seek advice from other practitioners if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
- Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. Under the GDPR and Data Protection Act 1998, you may still share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgment on the facts of the case. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to be shared.
- Consider safety and wellbeing: Base your information sharing decisions on considerations of the safety and wellbeing of the individual and others who may be affected by their actions.
- Necessary, proportionate, relevant, adequate, accurate, timely and secure: Ensure that information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).
- Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.