Version	Author/Owner	Drafted	Origin of Change / Comments	Changed by
1	Sarah Gibbon	M		

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.

This policy applies to anyone who has access to data and/or is [illegible]

e Data C roller ccasionally the person or more commonly the organisation with overa onsibil or the p essing ersonal data that organisation undertakes. They will make all the decisi about wh s cap d, how i sed and the purpose for it, as well as deciding what controls need to be ace.

is ally a perso t more comm by an organisation commissioned by a Data Co er to carry out ata processing behalf of the Data Controller. These are usually software pr rs such as Mic or contracted ervices 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.

means 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 data with our Data Processors, as these are processing it under our Data Controllership

- Reporting to the CEO or Principal, or in their absence the DPO in the following circumstances:
    - Any questions about the operation of this policy, data protection law, retaining or sharing personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;
    - If they are unsure whether they have a lawful basis upon which to use personal data in a particular way;
    - 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;
    - 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;
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
    - 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 - (section 10).

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
Comþ

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.

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.

This is not an absolute right.

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

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

The principles say that personal data must be:

-

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 ar n Gembï m

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:

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

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:

- Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law;
- 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;
- 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.

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.

A personal data breach is defined as

It may be

deliberate or accidental.

[redacted]

[redacted]

- 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
- Website defacement
- Hacking attack
- Unforeseen circumstances such as fire or flood
- Human error
- Breaches of policy such as
  - Server Room door left unlocked
  - Filing cabinets left unlocked
  - Temporary loss / misplacement of confidential or sensitive information or equipment on which data is stored

Near misses can include, but

guid... ake it n... y
and ... Miss... ures ... th

Reg... wil... staff to
and ... nd ... ces

W... e DPO ... on th
overall complia... data ... w, the
policy and for ... the data ... office

- 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

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.

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.

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 t

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about students and personal data about parents/carers.

The Priory Learning Trust is the 'data controller' for the purposes of data protection law.

Our data protection officer is One-West. E-mail One_West@bathnes.gov.uk

The categories of student information that we collect, hold and share about students include:

- Personal information (such as name, date of birth, unique pupil number, photograph and address)
- Characteristics (such as ethnicity, language, home language and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment and examination information (such as current, predicted and effort grades and internal/external examination results)
- Medical information (such as medical conditions, consent to store/administer medication, first aid administered and dietary needs)
- Special Educational Needs information (such as SEN status and need, diagnostic testing results and intervention received)
- Behaviour information (such as achievem s p

We will also share certain information about students aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our l nty we

The NPD is owned and managed by the Department for Education and co rmation a ents
in schools in England. It provides invaluable evidence on educational perfo nt
research as well as studies com by ment. It is held in ele
purposes. This information is secu nge of sources inc
and awarding bodies.

We are required by law, to provide udents to th ta
collections such as the school cen ar us. Som n is
NPD. The law that allows this is the bout u ngla ulati
2013.

To find out more about the NPD, g

You have a legal right to be informed about how our school uses any personal information that we hold about you. To comply with this, we provide a ‘privacy

Но

Once you reach the age of 16, we will [illegible] are certain information our local authority as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

You can contact our data protection officer to ask us to only pass your name, address and date of birth to our local authority.

Where we share data with an organisation that is based outside the United Kingdom, we will protect your data by following data protection law.

Your rights

How to access personal information we hold about you

You can find out if we hold any personal information about you, and how we use it, by making a , as long as we judge that you can properly understand your rights and what they mean.

[illegible]

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Some of the data we collect requires additional legal basis to process, and is known as Special Categories of Personal Data (SCoPD). The categories that we collect are:

- Racial or ethnic origin
- Biometric data for the purpose of uniquely identifying a natural person
- Trade union membership
- Data concerning health

There are additional legal bases for processing these special categories of personal data and these are laid out in our Data Protection Policy.

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to

T

If you would like to discuss anything in this privacy notice, please contact our Data Protection

Storing this information

We will keep your personal data while you are vis

We may also keep it beyond this, if necessary, to

Our record retention schedule sets out how long w

We do not share information about suppliers or the ent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it com information about you with:

- our local authority
- the Department for Education (DfE)
- Education service providers to enable them to p (such as academic websites for study purposes. Policy)

Where we transfer personal data to a country or territory outside accordance with data protection law.

a rig

Individuals have a right to make a to gain access to perse school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and it for
- Explain where we got it from, if
- Tell you who

To exercise any of these rights, please contact our data protection officer.

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

If you would like to discuss

Under data protection law, individuals have a right to be informed about how the Priory Learning Trust uses any personal data we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals applying for jobs at our Trust.

We, The Priory Learning Trust, Queensway, Weston super Mare, BS22 6BP are the 'data controller' for the purposes of data protection law.

Our data protection officer is officer is One-West (see 'Contact us' below).

Successful candidates should refer to our privacy notice for the school workforce for information about how their personal data is collected, stored and used.

We process data relating to those applying to work at our academies. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Copies of right to work documentation
- References
- Evidence of qualifications
- Employment records, including work history, job titles, training records and professional memberships

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Disability and access requirements

While the majority of the [redacted]n we collect from you is mandatory, there is some information that you can choose whether or n[redacted]ide to us.

Whenever we seek to co[redacted]mation from you, we make it clear whether you must provide this information (and if so, wh[redacted]ssible consequences are of not complying), or whether you have a choice.

If your application for em[redacted] is unsuccessful, the Trust or academy for which you have applied will hold your data [redacted] for 6 (six[redacted]

- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

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

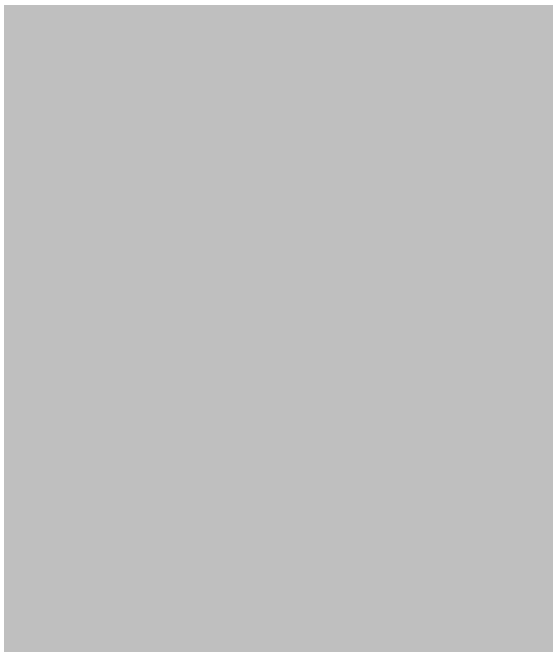
If there was any delay in reporting the incident, please explain why this was

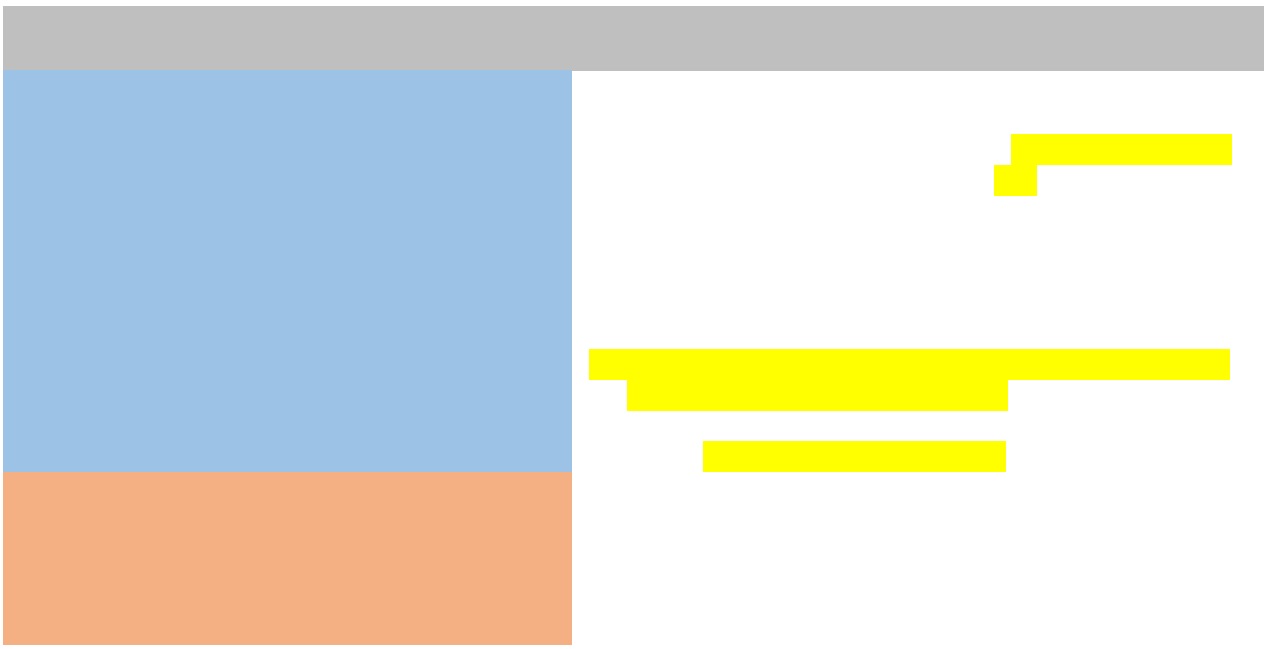
Include names of staff and data subject(s). Identifying information will be

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





Determine its scope, and involve the appropriate parties

Contain the incident to minimize its effect on other IT resources

Eliminate the affected elements

e.g. remove the malware and scan for anything remaining

Restore the system to normal operations, possibly via reinstall or backup.

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.

Que

- Yes / No

Based on:

Officer:

Signed: Date:

- Yes / No

Based on:

Officer:

Signed: Date:

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 cares” 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