DATA PROTECTION AND DATA BREACH POLICY

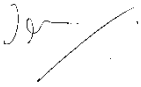
Policies approved by the Board of Trustees

Signed: 

Name: Katie Dominy **Date: 2nd September 2021**

Chair of Board of Trustees

Authorised for Issue

Signed: 

Name: Neville Coles **Date: 2nd September 2021**

Chief Executive Officer

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

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

Date policy adopted	September 2021
Review cycle	Annual
Review date	May 2022

Contents

1. Introduction……...4
2. Scope ……..4
3. Legal Principles ……4
4. Response Time in the Application of Legislation ……..6
5. Rights of Data Subject ……..6
6. Data Protection by Design ……7
7. Data Retention ……7
8. Data Breaches ……7
9. Complaints ……..7
10. Monitoring and Discipline ……9
11. Review ……9

Appendix 1 Subject Access Request Procedures ……10
Appendix 2 Privacy Notice for parents/carers ……11
Appendix 3 Privacy Notice for students (secondary schools only) …….15
Appendix 4 Privacy Notice for staff ……...18
Appendix 5 Privacy Notice for PRC ……..22
Appendix 6 Privacy Notice for visitors ……..24
Appendix 7 Data Sharing ……27
Appendix 8 Data Breach Form ……..30
Appendix 9 Security Incident Management (SIM): Record of Work ……32

1. Introduction

TPLT issues this policy to meet the requirements incumbent upon them under The Data Protection Act 2018 for the handling of personal data and Special Categories of Personal Data in the role of controller. If appropriate it can also be used for the control and release of data under the Freedom of Information Act 2000.

2. Scope

This policy applies to all employees of TPLT including contract, agency and temporary staff, volunteers and employees of partner organisations working for TPLT.

Special Categories of Personal Data (formerly known as Sensitive Personal Data) requires additional legal basis to process, along with additional protections.

The categories of data within scope of this policy are personal data revealing:

a) racial or ethnic origin
b) political opinions
c) religious or philosophical beliefs
d) trade union membership
e) genetic data
f) biometric data for the purpose of uniquely identifying a natural person
g) data concerning health; or
h) data concerning a natural person's sex life or sexual orientation

TPLT will set out the types of special categories of personal data it processes on data subjects in its Privacy Notices which are available on its website or by contacting any of our academies. It will also include the processing on its Information Audit which is updated annually.

3. Legal Principles

In execution of this policy TPLT will comply with the data protection principles of the GDPR specified in Article 5. These are that personal data be:

a) processed **lawfully, fairly and in a transparent manner** in relation to individuals;

b) collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;

d) **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits **identification of data subjects for no longer than is necessary** for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the law in order to safeguard the rights and freedoms of individuals;

f) processed in a manner that **ensures appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

TPLT will adopt the appropriate technological and organisational measures to ensure compliance with the Data Protection Principles by carrying out the necessary procedures. The concept of *data protection by*

design will be a guiding principle in achieving the security of individual's data protection rights. Reference should be made the Information Security Policy to ensure full compliance.

In all aspects of our work we will ensure that the rights of the data subject are protected by all practicable measures associated with the conduct of our work. The rights of the data subject as defined in law are;

a) The Right to be informed in a clear, concise and transparent manner
b) The Right of access
c) The Right to rectification
d) The Right to erasure
e) The Right to restrict processing
f) The Right to data portability
g) The Right to object
h) Rights related to automated decision making

In addition to the legal basis to process personal data, special categories of personal data will also requires an additional legal basis for processing. These are:

a) the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes.

It should also be noted that if TPLT offers an online service directly to a child, children aged 13 or over will provide their own consent. For children under this age explicit consent will be sought from whoever holds parental responsibility for the child, unless the online service offered is a preventive or counselling service.

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**;

c) processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a **foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim** and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e) processing relates to personal data which are **manifestly made public by the data subject**;

f) processing is necessary for the **establishment, exercise or defense of legal claims** or whenever courts are acting in their judicial capacity;

g) 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.

- Statutory and government purposes
- Administration of Justice and parliamentary purposes
- Equality of opportunity or treatment
- Preventing or detecting unlawful acts
- Protecting the public against dishonesty
- Journalism in connection with unlawful act and dishonesty
- Preventing fraud
- Processing for the purposes of preventing fraud.
- Suspicion of terrorist financing and money laundering
- Counselling
- Insurance
- Occupational pensions
- Political parties
- Elected representatives responding to requests

- Disclosure to elected representative
- Informing elected representatives about prisoners
- Publication of legal judgements
- Anti-doping in sport
- Standard of behaviour in sport

h) 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 UK law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i) processing is necessary for reasons of **public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of UK law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j) processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes** in accordance with Article 89(1) based on UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

4. Response Times in the Application of Legislation

In applying these regulations TPLT is obliged to adhere to the following schedules. The procedures for subject access are detailed in Appendix 1.

a) Subject Access Requests (SARs) whereby an individual may request personal information held by TPLT about themselves or a nominated individual on their behalf must be responded to within 1 month,

b) Where the above is found to be complex or numerous an extension may be granted allowing an additional 1 month however the subject must be informed within 1 month of their request,

c) No fee shall be charged for the above except where it is found to be excessive, repetitive or manifestly unfounded in accordance with the law,

IF APPROPRIATE

d) Freedom of Information Act Requests (FOIAs) whereby an individual may request information held by the council but may not contain information relating to individuals, subject to certain exceptions, must be responded to as soon as possible within 20 working days,

e) No fee shall normally be charged for the above. However in exceptional circumstances a fee may be charged,

f) Environmental Information Regulation requests (EIR) must be responded to as soon as possible but within 20 working days,

g) No fee shall be charged for the above.

5. Rights of the Data Subject

Where consent has been sought as the justification on processing, adequate measures must be in place to record consent and an appropriate method of removing the individual's personal data should consent be revoked must be adopted. In the vast majority of data processing activities a statutory power will be the reason for data processing.

Except where a statutory exemption applies or is in the public interest regarding health an individual who wishes to exercise their right to erasure shall have their personal data removed from all areas where applicable.

An individual when making a SAR is entitled to the following;

a) confirmation that their data is being processed;

b) access to their personal data;

c) other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

6. Data Protection by Design

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 TPLT will consult with its Data Protection Officer assess risks based on an initial screening process. 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.

Upon completion of a DPIA the regulator (ICO) maintains the right to cease the proposed processing should it remain high risk. Reference should be made the Information Security Policy to ensure full compliance.

7. Data Retention

Except where a specified retention period has been defined in accordance with the purpose of the activity any period of retention is defined by TPLT record retention schedule. This is detailed in the Information Retention Schedule.

8. Data Breaches

Appropriate measures are implemented to protect personal data from incidents (either deliberately or accidently) to avoid a data protection breach that could compromise security. A data breach is defined as the compromise of information's confidentiality, integrity, or availability which may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

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
    - Server Room door left open
    - Filing cabinets left unlocked

- 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 7, which is sent to the individual school's Business Manager who will liaise with its Data Protection Officer (One-West, contact on One-West@bathnes.gov.uk). A separate form, "TPLT Data Breach Reporting Form" is available to aid communication.

The organisation's lead officer shall complete the following phases of SIM (which are detailed in Appendix 8) 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.

9. Complaints

Where an individual makes a complaint relating to the processing of their personal data or is unhappy with any response to an SAR, FOI or EIR (if appropriate) request they may request an internal review (IR) be conducted. Requests for an IR should be within 40 days of the original response. The responsibility for the conduct of an IR is with the Trust who will discuss with the appointed DPO (One-West). The Trust contact is:

Sarah Gibbon
Chief Analytics Officer
The Priory Learning Trust
Queensway
Weston-super-Mare
BS22 6BP

If an individual is unhappy with the outcome of the IR they have the right to appeal to the Information Commissioner's Office (ICO) for assessment, the ICO is contactable at;

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

10. Monitoring and Discipline

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.

11. Review

This policy is reviewed annually by the Trust, when there is a change of Data Protection Officer or a change of Legislation 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.

Appendix 1 – 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 its Data Protection Officer, One-West (One-West@bathnes.gov.uk).

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 2: Privacy Notice for parents/carers

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 achievement, behaviour and exclusions)
- Family contact information (such as parents/carers names, addresses and contact numbers)
- Biometric fingerprint information (used for cashless catering system with separate consent required)
- CCTV images captured in school

Why we collect and use this information

We use the student data:

- to support student learning
- to monitor and report on student progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to safeguard students

The lawful basis on which we use this information

We only collect and use students' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process students' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use students' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using students' personal data overlap, and there may be several grounds which justify our use of this data.

Special Categories of Personal Data

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
- 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 student information

Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain student information to us or if you have a choice in this.

Storing student data

We hold student data while they are on roll. We may also keep it beyond their time on roll if this is necessary in order to comply with our legal obligations. Our Records Management Policy sets out how long we keep information about students.

Who we share student information with

We routinely share student information with:

- schools that the students attend after leaving us
- our local authority
- the Department for Education (DfE)
- Examining bodies
- Education service providers to enable them to provide the service we have contracted them for (such as academic websites for study purposes. Full details contained within our Data Protection Policy)

Why we share student information

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.

We share students' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our students with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services - Students aged 13+

Once our students reach the age of 13, we also pass student information to 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:

- youth support services
- careers advisers

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / student once he/she reaches the age 16.

Youth support services - Students aged 16+

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 local authority website.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about students in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our students to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our students from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to student information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.
For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided student information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Transferring data internationally

Where we transfer personal data to a country or territory outside the United Kingdom, we will do so in accordance with data protection law.

Requesting access to your personal data

Under data protection legislation, parents/carers and students have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact our Data Protection Officer, One-West. E-mail One-West@bathnes.gov.uk

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact our Data Protection Officer, One-West. E-mail One-West@bathnes.gov.uk

Appendix 3: Privacy Notice for Students (for students aged 12 and above)

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 notice' to you where we are processing your personal data.

This privacy notice explains how we collect, store and use personal data about you.

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 personal data we hold

We hold some personal information about you to make sure we can help you learn and look after you at school.

For the same reasons, we get information about you from some other places too – like other schools, the local council and the government.

This information includes:

- your contact details
- your test results
- your attendance record
- your characteristics, like your ethnic background or any special educational needs
- any medical conditions you have
- details of any behaviour issues or exclusions
- photographs
- CCTV images
- biometric fingerprints for paying for school dinners

Why we use this data

We use this data to help run the school, including to:

- get in touch with you and your parents when we need to
- check how you are doing in exams and work out whether you or your teachers need any extra help
- track how well the school as a whole is performing
- look after your wellbeing

Our legal basis for using this data

We will only collect and use your information when the law allows us to. Most often, we will use your information where:

- we need to comply with the law
- we need to use it to carry out a task in the public interest (in order to provide you with an education)

Sometimes, we may also use your personal information where:

- you, or your parents/carers have given us permission to use it in a certain way
- we need to protect your interests (or someone else's interest)

Where we have got permission to use your data, you or your parents/carers may withdraw this at any time. We will make this clear when we ask for permission, and explain how to go about withdrawing consent.

Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which means we can use your data.

Collecting this information

While in most cases you, or your parents/carers, must provide the personal information we need to collect, there are some occasions when you can choose whether or not to provide the data.
We will always tell you if it's optional. If you must provide the data, we will explain what might happen if you don't.

How we store this data

We will keep personal information about you while you are a student at our school. We may also keep it after you have left the school, where we are required to by law.

We have a Records Management Policy which sets out how long we must keep information about students.

Data sharing

We do not share personal information about you with anyone outside the school without permission from you or your parents/carers, unless the law and our policies allow us to do so.

Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

- schools that the students attend after leaving us
- our local authority
- the Department for Education (DfE)
- Examining bodies
- Education websites or apps which need your details to obtain log-in information

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The National Pupil Database (NPD)

We are required to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.

Some of this information is then stored in the National Pupil Database, which is managed by the Department for Education and provides evidence on how schools are performing. This, in turn, supports research.

The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.

The Department for Education may share information from the database with other organisations which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.

You can find more information about this on the Department for Education's webpage on how it collects and shares research data (https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information).
You can also contact the Department for Education if you have any questions about the database (https://www.gov.uk/contact-dfe).

Youth support services - Students aged 13+

Once you reach the age of 13, we are legally required to pass on certain information about you to 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.

Your parents/carers, or you once you are 16, can contact our data protection officer to ask us to only pass your name, address and date of birth to our local authority.

Youth support services - Students aged 16+

Once you reach the age of 16, we will also share 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.

Transferring data internationally

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 **'subject access request'**, as long as we judge that you can properly understand your rights and what they mean.

If we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you or your parents
- Tell you who it has been, or will be, shared with
- Let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- Give you a copy of the information

You may also ask us to send your personal information to another organisation electronically in certain circumstances.
If you want to make a request please contact our data protection officer.

Your other rights over your data

You have other rights over how your personal data is used and kept safe, including the right to:

- Say that you don't want it to be used if this would cause, or is causing, harm or distress
- Stop it being used to send you marketing materials
- Say that you don't want it used to make automated decisions (decisions made by a computer or machine, rather than by a person)
- Have it corrected, deleted or destroyed if it is wrong, or restrict our use of it
- Claim compensation if the data protection rules are broken and this harms you in some way

Complaints

We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we have done something wrong.

You can make a complaint at any time by contacting our Data Protection Officer. You can also complain to the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer, One-West. E-mail One-West@bathnes.gov.uk

Appendix 4: Privacy Notice for Staff

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 individuals we employ, or otherwise engage, to work at our school.

We, The Priory Learning Trust, are 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 school workforce information that we collect, process, hold and share include:

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

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Contract information, start dates, hours worked, post and role
- Bank account details, payroll records, National Insurance number, tax status information and employee/teacher number
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data and reasons for absence
- Copy of driving licence
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system

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
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we collect and use this information

The purpose of processing this data is to help us run the school, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Enable the development of a comprehensive picture of the workforce and how it is deployed
- Support the work of the School Teachers' Review Body

The lawful basis on which we process this information

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

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)

Special Categories of Personal Data

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 comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.
Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our Records Management Policy

Who we share this information with

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- our local authority
- the Department for Education (DfE)
- Education service providers to enable them to provide the service we have contracted them for (such as academic websites for study purposes. Full details contained within our Data Protection Policy)

Why we share school workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority
We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)
We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

We are required to share information about our pupils with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

Transferring data internationally

Where we transfer personal data to a country or territory outside the United Kingdom, we will do so in accordance with data protection law.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the Data Protection officer.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information

If you would like to discuss anything in this privacy notice, please contact our Data Protection Officer, One-West. E-mail One-West@bathnes.gov.uk

THE PRIORY
LEARNING TRUST

Appendix 5: Privacy Notice for PRC

Under data protection law, individuals have a right to be informed about how the PRC 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 members of the PRC.

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

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

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

- Personal information provided by you on joining (such as name, email address, date of birth and contact telephone number)
- We may also ask you for information when you report a problem with our site.
- If you contact us, we may keep a record of that correspondence.
- We may ask you to complete surveys that we use for research purposes, although you do not have to respond to them.
- Details of your visits to our site including, but not limited to, web server statistics, traffic data, location data and details of the web pages and resources that you access.

Colleting membership payments

We use Ashbourne Management to process payments for monthly membership fees. Members' names and direct debit information are given to Ashbourne Management on joining the PRC. We do not have access to any bank details through Ashbourne Management, and they have their own Privacy Notice on how they use your personal data.

Bookings

All bookings are made through YourApp, which is linked to the Ashbourne Management system. The only personal data we have available on bookings is the member's name.

Storing members' data

Whilst you are a paid member, all information you provide to us is stored on our secure servers.

How we use your information

We use information held about you in the following ways:

- to provide you with information, products or services that you request from us or which we feel may interest you, where you have consented to be contacted for such purposes.
- to carry out our obligations arising from any contracts entered into between you and us.

We may also use your data to provide you with information about goods and services which may be of interest to you and we may contact you about these by email, SMS, post or telephone. If you do not want us to use your data in this way, please contact our Data Protection Officer (see below).

Disclosure of Information

We do not disclose your personal information to any third parties. If, during the course of our normal business, it became necessary to disclose any information (eg following an incident within the PRC), we would request your consent to do this.

Our use of IP addresses and cookies

We may collect information about your computer, including where available your IP address, operating system and browser type, for system administration and to analyse aggregate information. This is statistical data about our users' browsing actions and patterns, and does not identify any individual. For the same reason, we may

obtain information about your general internet usage by using a cookie file which is stored on the hard drive of your computer. Cookies contain information that is transferred to your computer's hard drive. They help us to improve our site and to deliver a better and more personalised service.

They enable us:

- to estimate our audience size and usage pattern.
- to store information about your preferences, and so allow us to customise our site according to user needs.
- to speed up your searches.
- to recognise you when you return to our site.

You may refuse to accept cookies by activating the setting on your browser which allows you to refuse the setting of cookies. Unless you have adjusted your browser setting so that it will refuse cookies, our system will issue cookies when you log on to our site.

Your consent

By submitting your information you consent to the use of that information as set out in this policy. If we change our privacy policy we will post the changes on this page, and may place notices on other pages of the Website, so that you may be aware of the information we collect and how we use it at all times. We will also e-mail you should we make any changes so that you may consent to our use of your information in that way. If you wish to withdraw your consent for us to share your data, for example for marketing purposes outlined about, please contact info@theprc.org.uk.

Your Rights

You have the right to ask us not to process your personal data for marketing purposes. We will usually inform you (before collecting your data) if we intend to use your data for such purposes. You can exercise your right to prevent such processing by checking certain boxes on the forms we use to collect your data. You can also exercise the right at any time by contacting us. Our site may, from time to time, contain links to and from the websites of our clients and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

You have the right to withdraw this consent at any point and can do so by contacting the PRC directly on info@theprc.org.uk or by contacting our Data Protection Officer (see contact details below).

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information contact our Data Protection Officer, One-West. E-mail One-West@bathnes.gov.uk.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact our Data Protection Officer, One-West. E-mail One-West@bathnes.gov.uk.

Appendix 6: Privacy Notice for visitors

Under data protection law, individuals have a right to be informed about how the PRC 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 visitors to the school, in line with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

We, The Priory Learning Trust, are the 'data controller' for the purposes of data protection law. This means that we are responsible for deciding how we hold and use personal information about you.

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

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Name
- Contact details
- Information relating to your visit, e.g. your company or organisation name, arrival and departure time, car number plate
- Photographs for identification purposes for the duration of your visit
- CCTV images captured in school
- Information about any access arrangements you may need

Why we use this data

We use this data to:

- Identify you and keep you safe while on the school site
- Keep pupils and staff safe
- Maintain accurate records of visits to the school
- Provide appropriate access arrangements

The lawful basis on which we process this information

We only collect and use your personal data when the law allows us to. Most commonly, we process it where we need to comply with our legal obligation to keep our pupils and staff safe while on the school premises.

Less commonly, we may also process your personal data in situations where:

- We need it to perform an official task in the public interest
- We have obtained consent to use it in a certain way
- We need to protect someone's vital interests (save your life, or someone else's)

Where we have obtained consent, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how to withdraw it.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify our use of your data.

Collecting this information

Some of the information we collect from you is mandatory, and in some cases you can choose whether or not to provide the information to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

We will only collect the data that we need in order to fulfil our purposes, which are set out above.

Storing this information

We will keep your personal data while you are visiting our school.

We may also keep it beyond this, if necessary, to comply with our legal obligations.

Our record retention schedule sets out how long we keep information about visitors.

Who we share this information with

We do not share information about suppliers or their representatives, employees or agents without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- our local authority
- the Department for Education (DfE)
- Education service providers to enable them to provide the service we have contracted them for (such as academic websites for study purposes. Full details contained within our Data Protection Policy)

Transferring data internationally

Where we transfer personal data to a country or territory outside the United Kingdom, we will do so in accordance with data protection law.

Your rights

How to access personal information we hold about you

Individuals have a right to make a **'subject access request'** to gain access to personal information that the 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 processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our data protection officer.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by 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.

Complaints

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

Further information

If you would like to discuss anything in this privacy notice, please contact our Data Protection Officer, One-West. E-mail One-West@bathnes.gov.uk

Appendix 7: Data Sharing

TPLT and its Academies have a legal obligation to share data with the Department for Education, the Local Authority, examination awarding bodies, the Education and Skills Funding Agency, Ofsted, the Police Force and the Department for Health when lawful and appropriate. We also share data with a number of other organisations for educational or employment purposes, as shown in the table below:

Organisation	Reason for sharing	Information shared
Accelerated Reader (Hosted by Renaissance Learning)	Reading programme used to track students' progress in reading related to their chronological age	Student name, DOB, English class.
Access	Staff MIS	All staff data
ALICE	Library System	Student name, DOB, class, admission number
Bridgwater College (Year 11 only)	To ensure that Year 11 students have full information available to them during the transition to sixth form education	Student name, DOB, gender, address
Capita SIMS	Maintenance of main MIS system for students and staff. Data only visible during known maintenance periods	All student and staff data
Chartwells	School dinner provider	Student name, class, dietary requirements
Class Charts	To provide seating plans for teaching staff, recording of conduct data	Student name, year group, tutor group, UPN number, subject class, SEN, pupil premium, DOB, ethnicity
Classroom Monitor	Progress Tracking System	Student name, DOB, gender, FSM status, class, SEN status
Colorfoto	To facilitate the distribution of school photographs and the import of photographs onto the school Sims system	Student name, registration group, school admission number
CRB Cunninghams	Provision of school meals service, including biometric payment system. Provision of free school meals to appropriate students.	Student name, admission number, tutor group, gender, DOB, Year, Free school meal information, photograph, ethnicity, UPN. Biometric scan of finger/thumb taken once parental permission is received (no fingerprint is identifiable from this information) Staff name, gender, DOB
Delegated Services	Trip Health & Safety/Risk Assessments	Student name, staff name, potential personal details held in risk assessments – medical/contact information
Disclosure Barring Service	Vetting services for staff/volunteers/ contractors	Staff name, address, DOB, NI details, primary identity document detail, trusted government document detail, telephone numbers, nationality, previous addresses, previous names
Doddle	Homework/resources website	Student name, year group, class data, Parent user name, parent email, staff name, staff work email
Edenred	Childcare voucher Provider	Staff name, DOB, address, staff work email address, phone number, salary sacrifice deduction detail
The Education Broker (Capital Specialist Insurance Solutions Ltd)	Staff absence insurance	Staff name, doctors note detailing absence, DOB working hours/days, if staff member is pregnant, specifics of absence/operation

Elklan Training Ltd	Speech & Language Trainers – teacher training	Student name, academic information, photograph.
Exampro (Doublestruck Ltd)	GCSE data analysis tool for AQA exam boards	Student name, UPON, admission number, gender, DOB, year group, reg group, teacher name, class name, supervisor name, ethnicity, free school meal eligibility, SEN status, In Care status. Teacher name, job title, email, telephone.
Focus on Sound	Online music revision tool	Student name, username, hidden password (all created by student), test scores
Fusion 360	Computer Design Software	Student name, DOB, email
GCSEPod	GCSE revision website. By sharing data, the Academy is able to track how often students are accessing the revision materials and which topics are being studied	Student name, Unique Pupil Number, student e-mail address, DOB, gender, year group, group name, subject name, teacher. Staff name, work e-mail address, date of leaving, role, staff code.
Google G suite	To provide email, drive storage, calendars, google classroom and more	Staff and student name, student accounts are only activated once cloud permission form has been returned
HegartyMaths	Online maths teaching and learning tool	Student name, class, group, year, gender, UPN, DOB, leaving date. Staff name, email address
ICR Support for Schools	ICT Network support	Access to student name, staff name, correspondence
inVENTRY	Staff and visitor signing in and out, Fire evacuation. Staff data taken from Sims	Staff name, DBS data and personal information. Visitor name, car registration (if applicable), photograph – entered by visitor and stored on cloud service for 24 hours, then on internal servers for 12 months prior to deletion.
Kerboodle	Science homework/resources website	Student name, registration group, science class
Language Gym	Support for MFL teaching	Student name, email. Staff name, email
Liberata Teachers' Pension Scheme/Avon Pension Fund/South Gloucestershire Council	Staff pension service	Staff name, DOB, NI details, tax code, pay grade, salary, sickness records, pension information
Libresoft	Library System	Student name, DOB, class, admission number
Mathletics	Primary online maths system	Student name, lass, teacher's name
Mendip Vale Medical Group	Occupational Health Provider	Staff name, DOB, NI number, sickness record, address, phone number, email address. Data only shared on referral with consent
Microsoft Office 365	To provide access to Office 365 and apps	Staff and student name, school email address
My Maths	Maths revision site	Student name, maths class
No More Marking	English assessment tool	Student name, DOB, gender, year group, English class, pupil premium status, EAL
North Somerset Council	Tracking of student destinations post 16.	Student name, DOB, address, parent name, address, phone number
Pabulum Caterers	Provision of school meals service, including biometric payment	Student name, admission number, tutor group, gender, DOB, Year, Free school meal information, photograph,

	system. Provision of free school meals to appropriate students.	ethnicity, UPN. Biometric scan of finger/thumb taken once parental permission is received (no fingerprint is identifiable from this information) Staff name, gender, DOB
Parentpay	To facilitate payments into school for trips, events and other purchases	Student name, DOB, Gender, school admission number, Unique Pupil Number, tutor group, year group, parent name, address, telephone number, meal arrangements, eligibility for free school meals, ethnicity, religion, dietary needs, meal pattern Payments secured by Payment Card Industry Data Security Standard (PCIDSS)
PiXL English/Maths App	English and maths revision and practice questions	Student name, year group, English class, maths class. Students will be asked to enter an e-mail address when they first register for password reminders. Use of school e-mail address will be recommended.
PlanetArt (T/A FreePrint)	Printing of photographs	Photographs taken by staff for various student records
Provision Map – via Edukey	SEND tracking system	Student name, DOB, SEN Status, Ethnicity, EAL, Gender, FSM, LAC, PP, attendance, assessment results, photo, timetable. Staff name, email, role
PS Connect/Contact Group (Truancy Call/Parent Call)	Truancy Call is our absence call line for automated calls to parents if students not in school. Parent Call is used for reminders about parents evenings, Books4U and can be used in emergencies such as school closures	Student name, DOB, gender, school admission number, tutor group, ethnicity, religion, parent(s) name(s), parent(s) phone number(s), parent(s) e-mail address(es)
Reward Gateway (The PLaTform)	Staff benefit scheme/intranet	Payroll number, work e-mail address
Rising Stars & Mark System	Primary assessment data (PIRA/PUMA)	Student name, gender, DOB, class, test results
RM Unify	Staff email system (Castle Batch)	Staff name
SAGE	Finance Management System	Supplier and customer contact details
Scomis	Hosting of primary school SIMS system	All student and staff data
School Milk Service	Provision of milk to infant students	Student name
School Nurse Service	Vaccination records	Student name, DOB, address medical information
SISRA	Online data analysis tool (secondary)	Student name, exam number, tutor group, gender, ethnicity, SEN, FSM, LAC, pupil premium, attendance, assessment records
SNAP	Assessing the SEND needs for children	Student name, DOB, class, teacher's name, life event details, behavior information
South Gloucestershire County Council	Staff payroll service	Staff name, DOB, NI details, tax code, pay grade, salary, sickness records, pension information
Tapestry	EYFS online learning diary	Student name, DOB, gender
Tassomai	Science subject support	Student name, email. Staff name, email
Tempest	To facilitate the distribution of school photographs and the import	Student name, registration group, school admission number. Parent

	of photographs onto the school Sims system	contact information for ordering process.
Times Table Rock Stars	Maths resources	Student title, surname, forename, gender, classes, subjects, UPN
Teachers to Parents	Text message service	Student names, parent phone numbers
Vulnerable Learners (SSE)	SEN referrals	Student name, DOB, address, parent details, behavior/learning needs
Weston College (Year 11 only)	To ensure that Year 11 students have full information available to them during the transition to sixth form education	Student name, DOB, gender, address

TPLT will seek parental permission to set up a Google Apps for Education account in accordance with Google's terms and conditions.

From time to time the PLT and its Academies will participate in various on-line surveys, such as in-school questionnaires using websites such as SurveyMonkey, which are anonymous. We also facilitate some voluntary surveys (such as the Travelwest transport survey) where students may be requested to submit some personal details.

Appendix 8: 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 9 - 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	• 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: ○ 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.	
	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 **Decision to report to Data subjects** - Yes / No Based on: Officer: Signed: Date:
	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 significant economic or social disadvantage to the natural person concerned

	Decision to report to ICO - Yes / No Based on: Officer: Signed: Date: