

Data Protection Policy

This version effective from	15 June 2026
Policy will be reviewed	Annually
Policy provenance	Browne Jacobson
Policy editor	Head of Governance
Policy history	New version originated from Browne Jacobson to replace the previous Data Protection and Data Breach Policy approved by the TPLT Board on 18 July 2023.
Policy applies to	Priory Community School Worle Community School The King Alfred School Castle Batch Primary School Pawlett Primary School St Anne's Church Academy East Huntspill Primary School West Huntspill Primary School Berrow Primary Church Academy Burnham Infants School St Andrew's Church Junior School

1 **Policy statement**

- 1.1 Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as an academy trust (Trust”), we will collect, store, and **process personal data** about our pupils, **workforce**, parents, and others. This makes us a **data controller** in relation to that **personal data**.
- 1.2 We are committed to the protection of all **personal data** and **special category personal data**.
- 1.3 The law imposes significant fines for failing to lawfully **process** and safeguard **personal data**. This policy sets out how we comply with the relevant legislation. Breaches of this policy can result in the risk of real harm to individuals, action for damages, loss of trust and reputational harm as well as regulatory penalties, including fines.
- 1.4 All members of our **workforce** or other **data users** who process personal data on our behalf must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.
- 1.5 Where members of our workforce have a specific responsibility in connection with Processing, such as capturing consent, reporting a Personal Data Breach or conducting a Data Protection Impact Assessment as referred to in this Data Protection Policy or otherwise, then they must comply with the related policies and privacy guidelines.

2 **About this policy**

- 2.1 The types of **personal data** that we may be required to handle include information about pupils, parents, our **workforce**, and others that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in the retained EU law version of the General Data Protection Regulation ((EU)2016/679) (**‘UK GDPR’**), the Data Protection Act 2018, and other regulations (together **‘data protection legislation’**).
- 2.2 This policy and any other documents referred to in it set out the basis on which we will **process** any **personal data** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.
- 2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.
- 2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

3 **Definition of data protection terms**

All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in the Annex to this policy.

4 **Data Protection Officer**

- 4.1 As a Trust, we are required to appoint a Data Protection Officer (“DPO”). Our DPO is provided by OneWest and can be contacted by e-mail at One_west@bathnes.gov.uk.
- 4.2 The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.
- 4.3 The DPO is also the central point of contact for all data subjects and others in relation to matters of data protection.

5 Our data protection commitments

- 5.1 We are dedicated to ensuring that **personal data** is processed in alignment with the legal principles of data protection.
- 5.2 We implement a strategy focused on “Data Protection by Design and Default”.
- 5.3 We can prove our adherence to **data protection legislation**.
- 5.4 **Data subjects** are well informed about how and why we use their data, and they can exercise their rights regarding their data.
- 5.5 We share **personal data** only when it is fair and lawful, ensuring that any data sharing is conducted securely.
- 5.6 We manage and record all **personal data breaches**, including minor ones, effectively to mitigate any potential risks and to improve our practices. Where legally required we report serious breaches to the regulator (ICO) and other agencies where applicable.

6 Data protection principles

- 6.1 Anyone **processing personal data** must comply with the data protection principles. We will comply with these principles in relation to any **processing of personal data** by the Trust.
- 6.2 The principals provide that **personal data** must be:
 - 6.2.1 **Processed** fairly, lawfully, and transparently in relation to the **data subject**. This means that we only use **personal data** with respect for the individual who it relates to, in line with the legal grounds for **processing**, and we inform **data subjects on** how their **personal data** is **processed** including, among other ways, in our **privacy notices**.
 - 6.2.2 **Processed** for specified purposes and in a way which is not incompatible with those purposes. This means that if we collect **personal data** for one purpose and then we need to use it for another reason, we will ensure that new purpose is compatible with the original reason for **processing**.

- 6.2.3 Adequate, relevant, and not excessive for the purpose. This means that we will collect enough information to achieve our aim, whilst minimising that collection to what is genuinely required.
 - 6.2.4 Accurate and up to date. This means that we will try to ensure that **personal data** is accurate when we collect it and kept up to date over time.
 - 6.2.5 Not kept for any longer than is necessary for the purpose. This means that we will try to ensure that **personal data** is only kept for as long as is necessary to fulfil the purpose and according to our Records Retention Policy.
 - 6.2.6 **Processed** securely using appropriate technical and organisational measures. Our measures include; technical safeguards like security of ICT systems, control over ICT access, the use of pseudonyms and encryption, as well as organisational safeguards, including plans for business continuity, securing our premises and data physically, implementing policies and procedures, conducting regular training, and carrying out audits and evaluations of operational measures and strategic oversight of compliance.
- 6.3 **Personal data** must also:
- 6.3.1 Be **processed** in line with **data subjects'** rights.
 - 6.3.2 Not be transferred to people or organisations situated in other countries without adequate protection.
- 7 **Legal grounds for processing**
- 7.1 For **personal data** to be **processed** lawfully, it must be **processed** on the basis of one of the legal grounds set out in the **data protection legislation**. We will normally **process personal data** under the following legal grounds:
- 7.1.1 Where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract.
 - 7.1.2 Where the **processing** is necessary to comply with a legal obligation that we are subject to).
 - 7.1.3 Where the law otherwise allows us to **process** the **personal data**, or we are carrying out a task in the public interest.
 - 7.1.4 Where we are pursuing legitimate interests, (or these are being pursued by a third party), for purposes where they are not overridden because the **processing** prejudices the interests or fundamental rights and freedoms of **data subjects**; and
 - 7.1.5 Where none of the above apply, then we will seek the consent of the **data subject** to the **processing** of their **personal data**.

- 7.2 When **special category personal data** is being processed, then an additional legal ground must apply to that processing. We understand that for certain types of **processing of special category personal data**, we must have, and comply with, an appropriate policy document. Our special category personal data policy is our appropriate policy document for these purposes.
- 7.3 We will normally only **process special category personal data** under following legal grounds:
- 7.3.1 Where the **processing** is necessary for employment law purposes, for example, in relation to sickness absence.
 - 7.3.2 Where the **processing** is necessary for reasons of substantial public interest, for example, for the purposes of equality of opportunity and treatment or safeguarding vulnerable individuals at risk of harm.
 - 7.3.3 Where the **processing** is necessary for health or social care purposes, for example, in relation to pupils with medical conditions or disabilities; and
 - 7.3.4 Where none of the above apply, then we will seek the explicit consent of the **data subject** to the **processing** of their **special category personal data**.
- 7.4 We will inform **data subjects** of the above matters by way of appropriate **privacy notices**, which shall be provided to them when we collect the data, or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.
- 7.5 If any **data user** is in doubt as to the legal ground for processing **personal data** for any purpose, then they must contact the DPO before doing so.

Vital interests

- 7.6 There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** in order to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not able to give consent to the **processing**. We believe that this will only occur in very specific and limited circumstances. In such circumstances, we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

- 7.7 Where none of the other bases for **processing** set out above apply, then the Trust must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.
- 7.8 There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

- 7.9 When pupils join the Trust, a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate, third parties may also be required to complete a consent form.

8 **Data subjects' rights**

- 8.1 In addition to the right to be informed and the right to withdraw consent, we will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:

- 8.1.1 Request access to any **personal data** we hold about them.
- 8.1.2 Object to the **processing** of their **personal data**, including the right to object to direct marketing.
- 8.1.3 Have inaccurate or incomplete **personal data** about them rectified.
- 8.1.4 Restrict **processing** of their **personal data**.
- 8.1.5 Have **personal data** we hold about them erased.
- 8.1.6 Have their **personal data** transferred; and
- 8.1.7 Object to the making of decisions about them by automated means.

- 8.2 The DPO must be consulted in relation to any data subject rights request.

The right of access to personal data

- 8.3 **Data subjects** may request access to the **personal data** we hold about them and which we are able to provide based on a reasonable and proportionate search for that **personal data** and subject to any applicable exemptions from disclosure in the data protection legislation. Such requests will be considered in line with the Trust's subject access request procedure.

Data protection by design and default

- 8.4 The Trust will consider and comply with the requirements of **data protection legislation** in relation to all its activities whenever these involve the use of **personal data**, in accordance with the principles of data protection by design and default.
- 8.5 In certain circumstances, where the law requires us to, we shall carry out detailed assessments of proposed processing in a **data protection impact assessment** ("DPIA"). This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing**, or there is a change in our existing ways of working.
- 8.6 The Trust will complete a **DPIA** of any such proposed **processing**, and has a template document, which ensures that all relevant matters are considered.

- 8.7 The DPO should always be consulted as to whether a **DPIA** is required, and if so, how to undertake that assessment.

9 **Data security**

- 9.1 We will take appropriate security measures against unlawful or unauthorised processing of **personal data**, and against the accidental loss of, or damage to, **personal data**.
- 9.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.
- 9.3 Security procedures include:
- 9.3.1 **Entry controls** and a digital sign-in system for staff and visitors.
 - 9.3.2 **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (**Personal data** is always considered confidential.)
 - 9.3.3 **Methods of disposal.** Paper documents should be disposed of securely according to our confidential waste procedures. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the **ICO** guidance on the disposal of IT assets.
 - 9.3.4 **Equipment. Data users** must ensure that individual monitors do not show confidential information to passers-by, and that they log off from their PC when it is left unattended.
 - 9.3.5 **Document printing.** Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.
- 9.4 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

10 **Personal data breaches**

- 10.1 The Trust recognises that a breach of **personal data** could happen, despite our policies, procedures, and measures in place to protect **personal data**, and we will respond to any breach as quickly as possible in order to minimise any risks or potential harm to individuals.
- 10.2 The Trust has a personal data breach procedure, and this must be followed in relation to any actual or suspected breach of **personal data**.

11 **Disclosure and sharing of personal information**

- 11.1 We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, Ofsted, health authorities and professionals, the local authority, examination

bodies, other schools, and other organisations where we have a lawful basis for doing so.

- 11.2 The Trust will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.
- 11.3 Where necessary, we will enter into a data sharing agreement to help facilitate the safe sharing of **personal data**.

12 **Data processors**

- 12.1 We contract with various organisations who provide services to the Trust. These include people, companies, and systems that process personal data on our behalf and under our instruction.
- 12.2 In order that these services can be provided effectively, we are required to transfer **personal data** of **data subjects** to these **data processors**.
- 12.3 **Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust. The Trust will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.
- 12.4 Contracts with **data processors** will comply with data protection legislation, and contain explicit obligations on the **data processor** to ensure compliance with the data protection legislation, and compliance with the rights of **data subjects**.

13 **Images and videos**

- 13.1 Parents and others attending Trust events are allowed to take photographs and videos of those events for personal and domestic purposes. For example, parents can take video recordings of a school performance involving their child. The Trust does not prohibit this as a matter of policy.
- 13.2 The Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Trust to prevent.
- 13.3 The Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media, or otherwise publish those images or videos.
- 13.4 Whenever a pupil begins their attendance at the Trust, they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. Images and videos of pupils may be required for safeguarding, assessment and learning purposes and we will not seek consent for the taking and use of these images. However, as a Trust we want to celebrate the achievements of our

pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

14 **Video surveillance**

The Trust operates a CCTV system. Please refer to the Trust CCTV policy/video surveillance policy.

15 **Biometric data**

15.1 The Trust operates a **biometric recognition system** for the purpose of:

- Payment of dinner monies.

Before we are able to obtain the **biometric data** of pupils or the **workforce** we are required to give notification and obtain consent for this **special category data** due to additional requirements for processing such data under the **data protection legislation** and/or Protection of Freedoms Act 2012.

15.2 For the **workforce**, explicit written consent will be obtained at the commencement of their position within the Trust and shall continue to be effective unless an objection in writing to the processing of the **biometric data** is received from the individual.

15.3 For pupils under the age of 18 years, the respective School will notify each parent of that pupil (that the School has the contact details for, and is able to contact) prior to them commencing their education at the school, of the use of our **biometric recognition system**. The School will then obtain the written consent of one of the pupil's parents before obtaining any **biometric data**.

15.4 In the event that written consent cannot be obtained from a parent, or any parent objects in writing, or the pupil objects or refuses to participate in the processing of their **biometric data**, the Trust will not process the pupil's **biometric data** and will provide alternative means of accessing the above services.

15.5 Further information about this can be found in our notification of intention to process pupil's biometric information and our **privacy notices**.

16 **Complaints**

16.1 **Data subjects** have the right to make a complaint to the Trust if they consider we have not complied with **data protection legislation**. Any complaints relating to data protection must be directed to our **DPO**.

16.2 When dealing with complaints relating to data protection, we shall:

- 16.2.1 Acknowledge receipt of the complaint within 30 days of the date on which the complaint is received by the Trust;

16.2.2 Take appropriate steps to respond to the complaint, including making enquiries into the subject matter of the complaint, to the extent appropriate;

16.2.3 Inform the complainant about progress of the complaint; and

16.2.4 Inform the complainant of the outcome of the complaint.

17 **Changes to this policy**

We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

ANNEX

DEFINITIONS

Term	Definition
Biometric data	Is information about a person's physical or behavioural characteristics or features that can be used to identify them and is obtained or recorded for the purposes of a biometric recognition system and can include fingerprints, hand shapes, features of the eye/facial recognition, or information about a person's voice or handwriting.
Biometric recognition system	Is a system that operates automatically (electronically) and: • Obtains or records information about a person's physical or behavioural characteristics or features; and • Compares or otherwise processes that information with stored information in order to establish or verify the identity of the person, or otherwise determine whether they are recognised by the system.
Data	Is information, which is stored electronically on a computer, or in certain paper-based filing systems.
Data subjects	For the purpose of this policy includes all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Personal data	Means any information relating to an identified or identifiable natural person (a data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data controllers	Are the people who, or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with data protection legislation. We are the data controller of all personal data used in our business for our own commercial purposes.

Data users	Are those of our workforce (including governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy, and any applicable data security procedures, at all times.
Data processors	Include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Data protection legislation	Means all applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR and the Data Protection Act 2018 (DPA 2018) (and regulations made thereunder) (as amended by the Data (Use and Access) Act 2025; and the Privacy and Electronic Communications Regulations 2003 (SI 2003 No. 2426) as amended, and all other legislation and regulatory requirements in force from time to time which apply to the use of personal data.
Data protection impact assessment (DPIA)	A tool to help identify how to comply with data protection obligations and protect individuals' rights as set out in Article 35 of the UK GDPR. The ICO also has guidance on DPIAs on their website at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/ .
Information Commissioner's Office (ICO)	in the UK, the Information Commissioner's Office (ICO) is the data protection regulator. The website of the ICO is at www.ico.org.uk .
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.
Privacy notices	Where we collect information either directly or indirectly from data subjects, we provide them with a statement of fair processing, referred to as a privacy notice. This notice will contain information about: our identity and contact details as data controller and those of the DPO, the purpose, or purposes, and legal basis for which we intend to process that personal data, the types of third parties, if any, with which we will share, or to which we will disclose that personal data, whether the personal data will be transferred outside the UK and if so, the safeguards in place, the period for which their personal data will be stored, by reference to our [data retention policy], the existence of any automated decision making in the processing of the personal data along with the significance and envisaged

	consequences of the processing and the right to object to such decision making, and the rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.
Processing	Is any activity that involves use of the data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.
Special category personal data	Includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, sexual orientation or genetic or biometric data.
Workforce	Includes any individual employed by the Trust such as staff and those who volunteer in any capacity including Trustees/members/local governors/community councillors/parent helpers.