

# DATA PROTECTION POLICY

## **Mission Statement**

WeST holds a deep seated belief in education and lifelong learning. Effective collaboration, mutual support and professional challenge will underpin our quest to ensure that all children and adults that we serve are given every opportunity to fulfil their potential and succeed in life.

Westcountry Schools Trust adopted this policy review in October 2021

Westcountry Schools Trust will review this policy in September 2023



### Westcountry Schools Trust Data Protection Policy Policy Statement

Westcountry Schools Trust is committed to protecting the rights of individuals with regards to the storing and processing of personal data. It has established the following policy to support this commitment.

Westcountry Schools Trust undertakes to apply this policy to all Westcountry Schools Trust sites and to ensure that its employees, contractors, agents or others processing information on behalf of Westcountry Schools Trust complies with their obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

The day to day management of data protection issues rest with the WeST Data Protection Team.

#### WeST Data Protection Team

The Data Protection Team consists of the WeST Data Protection Officer working with data protection lead officers for all WeST sites and the West Central Team.

The team will:

- Ensure that guidance is available on all matters relation to the UK General Data Protection Regulation and the Data Protection Act 2018
- Ensure the Trust board, head teachers / principals and data subjects are notified of changes to the Privacy notices in processing of personal data
- Report to the highest levels of management on data protection issues
- Deal with matters relating to Subject Access requests
- Deal with matters relating to Data Breach and notifications to the Information Commissioner's Office (ICO)

#### Introduction

The GDPR legislation is designed to 'harmonise' data privacy laws across Europe, as well as give greater protection and rights to individuals. The EU GDPR has been retained in UK law and will continue to be read alongside the Data Protection Act 2018.

Article 4 (1) of UK GDPR defines personal data as being:

- 'Any information relating to an identified or identifiable natural person' ('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'

Under EU GDPR legislation individual member states were able to make limited local adjustments in law. In the UK, the DPA 2018 is the detail of these specific adjustments. It is therefore important the UK GDPR and the DPA 2018 are referenced side by side.

Under UK GDPR and DPA 2018 legislation Westcountry Schools Trust, as the data controller and data processor, has a legal obligation to comply with the UK GDPR and DPA 2018.

Organisations **MUST** follow the 6 Data Protection Principles to ensure data is:

- Processed fairly, lawfully and in a transparent manner
- Used for specified, explicit and legitimate purposes
- Used in a way that is adequate, relevant and limited
- Accurate and kept up to date
- Kept no longer than is necessary
- Processed in a manner that ensures appropriate security of the data

In addition to these principles, there are 6 legal bases

- the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a **legal obligation** to which the controller is subject;
- processing is necessary in order to **protect the vital interests** of the data subject or of another natural person;
- processing is necessary for the performance of a **task carried out in the public interest** or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

### Processing personal information

The processing of personal information by Trust employees, contractors and agents must only be in the course of their official duties. Use for any other purpose is prohibited. The Trust will assess the appropriate level of security and ensure that any identified risks are minimised. Accidental or unlawful destruction, loss, alteration, unauthorised disclosure of personal data transmitted, stored or otherwise processed is strictly forbidden and may constitute a criminal and/or a disciplinary offence.

Westcountry Schools Trust processes personal data as it is necessary to carry out tasks in the public interest. Therefore, details of what data we collect, hold and disclose **MUST** be shown in our Privacy notices. Any amendments to the privacy notice need to be disclosed

in advance of obtaining information. Training will be provided to ensure that all processing activities are undertaken in line with legal requirements and Westcountry Schools Trust guidance.

Westcountry Schools Trust, through its schools, will seek consent to use any data not subject to processing under "public interest" or in the "performance of a contract". Specific consent will be required for any additional uses of data e.g. photographic images for use on school publications. Consent is required to be specific and can be withdrawn at any time.

### Security in the work place

Access to any working area or IT equipment must be restricted to employees, contractors and agents in the course of their official duties. Identification badges must be worn at all times and individuals found not wearing an identification badge should be challenged. Any visitors or contractors entering any work area or using any IT equipment must be accompanied at all times.

A **clear desk policy** will be adopted in order to reduce any potential unauthorised access to paper records containing personal information.

A **clear screen policy** will be adopted in order to reduce any potential unauthorised access to any IT systems.

All **IT equipment is password protected** in order to keep data secure.

The following **password policy** is suggested - IT users have to create their own password in order to log onto IT equipment. Passwords should be changed regularly. Passwords need to be difficult for others to guess so family/pets names should be avoided. Passwords should contain a combination of upper and lower case letters and numerals which should be changed if you suspect ANYBODY knows your password. You will be forced to change your password if your password is known to be compromised. Passwords must not be written down or disclosed to anyone else.

**Use of Trust email accounts** – Trust / school email accounts will be provided to all staff (including governors and trustees) to enable effective communication in line with the requirements of the role. These email accounts should not be used for personal business and are subject to scrutiny under right of access requests that may be received from data subjects.

**Removable media MUST be encrypted** – the use of removable media is not recommended to transfer or transport personal or sensitive data that, if accessed unlawfully, might present a high risk to the rights and freedoms of the data subject. If there are no alternative options removable media MUST be encrypted.

### Disclosure of Information

Personal information held must not be disclosed to anyone internally or externally, unless the person disclosing the information is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled to the information. Guidance should be sought from the Data Protection Team when verification of this is not possible.

In the case of any doubt concerning the disclosure of personal information, advice can be sought from the WeST Data Protection Team.

### **Exemption from the Non-Disclosure Provisions**

There may be occasions when we need to disclose information about someone which will usually be in breach of the Data Protection Act 2018. For example, if we wanted to disclose information knowing that the disclosure would be likely to cause that person damage or distress (this is one of the non-disclosure provisions), the Data Protection Act contains exemptions which allow us to override a non-disclosure provision in certain circumstances, if the disclosure is in the public interest. Advice should be sought from the Data Protection Team in such matters.

### **Rights of Access to Personal Information**

Under Article 15 of the UK GDPR 'Rights of access by the data subject' every individual has the right to make a Subject Access Request (SAR) to any organisation to obtain a copy of all the data held on them. This could be specific data, or everything held.

On a request being received, the controller has one month to comply with this request. Schools are not exempt even in school holidays. On sight of such a request the Data Protection Team needs to be informed without delay.

Details on making a subject access request can be found on the WeST website.

### **Accuracy of Data**

It is the responsibility of those who receive personal information to ensure, so far as possible, that it is accurate, valid and up to date. Individuals who input or update information must also ensure that it is adequate, relevant, unambiguous and professionally worded. Matters of opinion (not fact) must be clearly recorded as such.

### **Review and Destruction of Data**

Any personal data held must be reviewed at frequent intervals to ensure that it is accurate, up to date and still relevant. If the personal data held is no longer needed and there is no legal or other reason for holding the information, it must be destroyed. Westcountry Schools Trust follows the guidance from the Information and Records Management Society please contact the Data Protection Team for further information.

### **The right to be forgotten 'erased'**

Under Article 17 of the UK GDPR individuals do have the right to have their data erased if requested. However, schools are slightly different – legally we have to retain the majority of

pupil information until their 25th birthday, however there are different timelines for some types of pupil records. For example: looked after children.

Any such requests need to be passed, in writing, to the Data Protection Team who will take the relevant actions required in line with the UK GDPR and DPA 2018.

### Data Breach

A personal data breach means a breach of security leading to the **accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to**, personal data. This includes breaches that are the result of accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. There will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

In the event of a data breach there are procedures in place that all Westcountry Schools Trust employees, contractors or agents should follow. It is a criminal offence to 'cover up' or try to hide a data breach. All data breaches, however small, should be discussed with the Data Protection Team and recorded as agreed. A central record of data breaches is held and will be regularly reported to the Trust board.

### Contacts

If you would like to discuss any element of this policy please contact the WeST Data Protection Officer at [DPO-west@westst.org.uk](mailto:DPO-west@westst.org.uk)

### Data Protection Regulation

The regulatory body for data protection matters in the UK is the Information Commissions Office. If you have a concern about the way WeST process 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/>

### ICO registration

As required by UK GDPR legislation Westcountry Schools Trust is registered with the ICO as a data controller.

Registration Number- Z3367281

Registered address: Harford Road, Ivybridge, Devon. PL21 0JA

Other names associated with this registration:

School name	School name
Ashburton Primary School	Morley Meadow Primary School
Atrium Studio School	Oreston Community Academy
Austin Farm Primary School	Plymstock School
Boringdon Primary School	Plympton St Maurice Primary School
Buckfastleigh Primary School	Sherford Vale School
Callington Community College	Stowford School
Chaddlewood Primary School	South Dartmoor Community College
Coombe Dean School	The Learning Institute
Eggbuckland Community College	Ugborough Primary School
Ermington Primary School	Wembury Primary School
Glen Park Primary School	Woodford Primary School
Hele's School	Woodlands Park Primary
Holbeton Primary School	Yealmpton Primary
Ivybridge Community College	Westcountry Schools Trust
Manor Primary School Ivybridge	

**Data Protection Policy 2021/22**

Staff and Governor sign off

Agreement I the undersigned, confirm that I have read, and agree to comply with, the terms and conditions of the Westcountry Schools Trust Data Protection Policy.

**Print Name** .....

**Signature** .....

**School/Setting** .....

**Date** .....

Please complete the above details, scan this page and email to your HR admin

