

GDPR POLICY AND PROCEDURE

Policy Number	HCT-GDPR-002
Version	2
Applicable To	Staff of Horizon Community Training (including volunteers and partners)
Document Owner	Kath Shanahan
Next Review	September 2027
Availability	Policies and Procedures Folder, SharePoint, Company Website

Introduction

Horizon Community Training CIC (Horizon) approach is that protecting the confidentiality and integrity of personal data is a key responsibility of all staff. As an organisation that collects, uses and stores personal data about its staff, suppliers (sole traders, partnerships or individuals within companies), learners, parents and visitors and other users of its services, Horizon recognises that having controls around the collection, use, retention and destruction of Personal data is important in order to comply with our obligations under Data Protection Laws and in particular its obligations under Article 5 of General Data Protection Regulation (GDPR).

This Policy and Procedure sets out the basis on which Horizon will collect and use personal data either where the establishment collects it from individuals itself, or where it is provided to us by third parties. It also sets out rules on how Horizon uses, transfers and stores Personal data. It applies to all personal data stored electronically, in paper form, or otherwise. For further details in terms of the collection, storage, protection and usage of personal data refer to Horizon's Privacy Policy.

Purpose

This Policy and Procedure describes how Horizon will ensure all staff are aware of what they must do to ensure the correct and lawful treatment of personal data.

Key Contacts

Name	Role	Email	Telephone
Katherine Shanahan	Data Protection Officer (DPO)	katherine@horizoncommunitytraining.co.uk	01493 717767
Information Commissioners Office (ICO)	ICO	Information Commissioner's Office	See website

Principles

All Horizon staff must comply with this Policy and Procedure. Horizon's general obligations are as below:

Horizon must ensure that all personal data that they collect, store, use and come into contact with during the performance of their duties is kept confidential.

Horizon staff must not release or disclose any personal data:

- Outside the establishment without permission from the DPO or
- Inside the establishment to Horizon members not authorised to access the personal data, without specific authorisation from the DPO; this includes but is not limited to by phone calls, text messages or in emails.

Horizon must take all steps to ensure there is no unauthorised access to personal data whether by other Horizon staff who are not authorised to see such personal data or by people outside the establishment.

When using personal data, Data Protection laws require that Horizon complies with the following principles. These principles require personal data to be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
- Accurate and kept up-to-date, meaning that every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified as soon as possible;
- Kept for no longer than is necessary for the purposes for which it is being processed; and
- 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.

In addition to complying with the above requirements Horizon also has to demonstrate in writing that it complies with them. Horizon has a number of policies and procedures (Safeguarding, Online Safety) in place, which help to ensure that Horizon can demonstrate its compliance.

Horizon has carefully assessed how it uses personal data and how it complies with the obligations set out above. If Horizon changes how it uses personal data, this policy and procedure will be updated.

Data Subjects Rights

There are a number of different Data Subject Rights as detailed below:

Access – Allows individuals to request confirmation that their personal data is being processed and to receive a copy of that personal data, along with information about how it is used. Access to personal data is usually made with a Subject Access Request (SAR).

A SAR allows individuals the right to obtain the following:

- Confirmation that their personal data is being processed
- A copy of their personal data
- The purpose for which the data is being used
- The categories of personal data being processed
- The recipients or organisations the data has been shared with
- How long the data will be stored
- Information about their data protection rights
- Details of any automated decision-making or profiling

Horizon must respond within one month of receiving a SAR. In complex cases, this may be extended by up to two additional months, according to guidance from the Information Commissioner's Office.

All SAR requests need to be in writing to the DPO and should specify exactly what information is being sought and over what time frame.

Rectification – Allows individuals to request that their personal data is changed/updated in the event that they feel that it is inaccurate. It also allows individuals to request that the use of their personal data is restricted.

Erasure – Allows individuals to request that their personal data is deleted by Horizon, where there is no justifiable reason as to why it should be retained.

Portability – Allows individuals to request that their personal data is presented to them in a structured, commonly used machine-readable format to enable them to share their data with other organisations.

Objection – Allows individuals to request that Horizon refrains from using their personal data for a specific purpose, such as for marketing purposes.

Should Horizon staff have concerns in respect to their Data Rights, they need to speak to the DPO.

Data Breach Reporting Process

All data breaches need to be reported to the DPO in writing and will need to include the below:

- Details of when and where the breach occurred
- Who was involved in/or responsible for the breach
- Did anyone witness/is witnessing the breach

Horizon will adhere to reporting requirements as set out by the ICO.

Security Measures

Horizon store personal information on computer servers in a controlled secure manner by adopting the below measures:

- A recognised internet service via an established communications company
- A Firewall and robust antivirus software
- An encrypted and password protected Wi-Fi network, using strong, unique passwords passcodes/passwords including Multi Factor Authentication (MFA) and screen locks on devices
- Having the latest operating system/security updates installed
- Any hard copies of personal information are kept in locked cabinets within a locked office

For further information in terms of the storage of information/records please refer to Horizon's Safeguarding Policy and Procedure.

Data Sharing

Horizon may receive a request to provide personal information to another organisation, third party, for example Government bodies or external agencies involved in the safeguarding of our learners. Horizon will ensure that any data sharing is completed in a fair and lawful manner, taking into account the below:

- There should be a valid and legitimate reason, such as service regulation or safeguarding requirement for the request
- Only the minimum information should be shared
- Permission should be sought from the individual whose personal information is being shared unless doing so would compromise a legal process

- The information should be shared securely, for example in a private phone call or via password protected encrypted email

Data protection law is not a barrier to sharing information when it is necessary, proportionate, and justified to do so. The most important consideration is to safeguard and promote the welfare of our vulnerable young people.

The Data Protection Act 2018 allows all organisations to process data for safeguarding purposes lawfully and without consent where necessary for the purposes of:

- protecting an individual from neglect or physical and emotional harm; or
- protecting the physical, mental or emotional wellbeing of an individual

The above covers situations where a learner may be at risk of significant harm due to neglect or abuse and applies to referrals made to the local authority for any learners considered to be a 'child in need'.

All personal information will be treated as confidential. However confidential information may be shared to other agencies to safeguard and promote the welfare of our vulnerable young people.

In some circumstances, seeking consent from a person we believe is neglecting or abusing a vulnerable young person may undermine safeguarding procedures and may increase the risk of harm to the young person or another person. In these situations, we will share this information without consent.

If a learner makes a disclosure, we will never promise the learner confidentiality, instead we will explain that the information will need to be passed on to the appropriate person to help keep them safe.

Horizon is responsible for lawfully sharing the information we hold, and we must not assume that someone else will pass on information that may be critical to safeguard and promote the welfare of a learner.

Our organisation will adhere to the following principles of information sharing:

- Information sharing must be necessary and proportionate to the circumstances of the young person
- The information must be shared quickly and securely
- Use clear and precise language
- Identify how the information is to be shared
- Record exactly what has been shared
- If information is withheld, then that should also be recorded

When sharing information with any organisation, we will first consider the principles outlined by Government Guidance. We will consult the 7 golden rules for information sharing from 'Information Sharing Advice for Safeguarding Practitioners'.

Data Retention

Horizon will destroy data securely as detailed below:

- Employment Records/Files/Information-6 years after employment ends
 - Job Applicant Details/Information-12 months after application is made
 - Learner Records/Information-(Inclusive of Safeguarding/Child Protection Data/Information- after learners 25th Birthday
-