



Data Protection And Information Security Policy

Most recent update: 17 May 2024

Aims

This policy statement is designed to set out the roles and responsibilities of protecting valuable information held by the Cheshire West and Chester (CW&C) Skills and Employment team. It will illustrate how existing procedures comply with data protection legislation, set out a framework for any new procedures and set out the selection and application of appropriate safeguarding techniques that will further help the storing of information securely.

Scope

The Skills and Employment team work in a wide range of areas including Adult Education, Family Learning, employment mentoring - including for those in primary or secondary mental health care - and Work Zone supported provision.

The following policies apply to all members of staff who have direct contact with data:

- The contracted provider - when returning data electronically by post or handing over in person. Full instructions are issued by the Skills and Employment's Quality Performance and Commissioning team and may be changed at short notice.
- Direct delivery teams - who must store personal records securely, either physically or electronically.
- Skills and Employment staff - receiving customer data, processing that data and disseminating reports to appropriate staff and contractors.

Customers' data cannot be shared with third parties unless explicitly specified (this is confirmed in the Privacy Notice at the beginning of the learner details form).

All areas of information processing, retention and disposal will be covered in this policy; from the customer entering their details onto a registration form, to the transfer of that information to central data inputters and finally how the data is analysed and stored on our systems. The policy will provide guidelines on efficient processes, such as how to store and finally destroy personal/sensitive data.

Policy Statement

This policy statement focuses on implementing reasonable systems and structures. Sufficient resources are put in place so that the security objectives can be realistically achieved.

Compulsory Data Protection training must be completed by all staff who handle data. Employees responsible for personal or sensitive data will also receive training appropriate to their role.

Unannounced examinations will be conducted by the manager to help develop ways in which security can be improved. Any Skills and Employment staff members who discover security





shortfalls will be responsible for reporting them to their line manager and following CW&C data protection breach procedures.

Staff will at all times act in a responsible, professional and security-aware manner, maintaining an awareness of this policy statement and General Data Protection Regulation principles.

This policy will be distributed via the relevant shared folders and www.cheshirewest.gov.uk website in order to be easily accessible by all Skills and Employment staff and subcontractors.

Legislative Influences

This policy is written in accordance with the 2018 Data Protection Act and General Data Protection Regulations (GDPR). It follows GDPRs six data protection principles which ensure that personal data is:

1. Processed lawfully, fairly and transparently,
2. Collected for specified, explicit and legitimate purposes,
3. Adequate, relevant and limited to what is necessary for processing,
4. Accurate and kept up to date,
5. Kept in a form that allows for the identification of data subject only as long as necessary,
6. Processed in a manner that ensures its security.

Personal Data

GDPR applies to *personal data* meaning any information relating to a person who can be identified directly or indirectly. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification numbers, location data or online identifiers. This reflects changes in technology and the way organisations collect information about people.

GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive Personal Data

GDPR refers to sensitive personal data as “special categories of personal data”.

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Special category data would also include the health data that Skills and Employment staff collect from customers, including any family history of health conditions including mental health conditions.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.



Individual Rights

GDPR states that the customer must have clear and understandable information of what their data is going to be used for and how it is going to be stored. The regulations also strengthen an individual's right to be forgotten if the information previously obtained is no longer necessary, or the storage period consented has expired.

Skills and Employment provision is delivered either directly or through its subcontractors. It could be funded by the Department for Education (DfE), National Health Service (NHS) or Department for Work and Pensions (DWP). The legal basis for all Skills and Employment provision is 'public task' as the processing of customers' data is necessary for CW&C to perform official duties relating to a function which has a clear basis in law. This covers the majority of customer data collected by the Skills and Employment team, however there may be some smaller programmes which rely on consent or contract as a legal basis and consequently customers will have different rights for those programmes.

The table below outlines the rights associated with each legal basis.

	Right to erasure	Right to portability	Right to object
Consent			x but right to withdraw consent
Contract			x
Legal obligation	x	x	x
Vital interests		x	x
Public task	x	x	
Legitimate interests		x	

As a result of this legal basis CW&C's DfE, NHS and DWP funded customers do not have a right to erasure or portability. This legal basis is clearly set out in the learner registration privacy notice.

The privacy notice also clearly sets out why CW&C collects customer data, how CW&C processes that data, the conditions where a customer's data may be shared, and the customer's rights with regard to their data and how long their data will be stored.

CW&C customer data is stored in accordance with the reason for collecting and storing that data, normally relating to a public contract being fulfilled. Some Skills and Employment programmes were funded by the EU. Any such courses between 2014 and 2019 will have records held until the end of March 2027. All records for courses from 1 February 2020 onwards will be held for 6 years.



Right Of Access To Information

Section 11 of the Human Rights Act 1998 safeguards the right to ask for personal information¹, making it vital to store data in a secure, well organised manner which can be easily accessible only by those who are authorised to do so. This policy will focus on the Information Commissioners Office (ICO) Code of Practice. A request for information must be made in writing, must be accompanied by proof of identity and proof of address. All information must then be provided within forty days of receiving the complete request.

Policy In Practice

Data security is not simply a matter of paper, databases, servers and storage facilities. It relates to the complete management information system. This makes it difficult to provide complete data security for any organisation. 'Total and complete network security are seen as a myth'², therefore this information security statement will merely propose policy guidelines that can be implemented to limit unauthorised accessing of data. Complete security in every case cannot be guaranteed. Any specific incident will be left to the discretion of the line manager who will follow CW&C data protection procedures.

Our Privacy Notice



Privacy Notice.pdf

¹ Pg 7 Ch2 'Data Protection and Human Rights' – House of Lords & House of Commons Joint Committee on Human Rights, 14th report of session 2007-2008, printed 4th March 2008

² 'Security as a Process' - Mastering Network Security (2nd edition) – Chris Brenton, Camron Hunt



Policy guidelines that can be used to maximise data protection

When working with hard copy data

- Data should be well organised, clearly labelled and easily accessible by those who are authorised to do so.
- Records should be stored in lockable storage facilities, located areas or offices that are not normally accessible to the public; there should be at least two locks between the public and the hard copy data.
- If it is not reasonable for those transferring records to return records straight to a main data storage area, the person transporting the records should:
 - Inform their line manager or the local data controller of the number of records they are transporting and when they will be returned to a main storage facility
 - Ensure that the case, which the records are being transported in, is not left visibly unattended at any point during the transfer
 - Ensure that while storing records outside of a main storage facility, reasonable steps are made to ensure that the storage case is left in a secure, non-visible location
- If physical transfer of significant numbers of unencrypted paper records be necessary, two persons should oversee the transfer at all times.
- A register of transfers of significant numbers of unencrypted paper records should be taken at the departure and receiving end of the transfer, this register should not be overseen by those transferring the records.
- Records will finally be destroyed by being disposed of in a locked metal container, then shredded only by those who are authorised to do so.

When working with electronic data

- Electronic records should only be transferred over the internet using a secure connection (the padlock should be shown at the bottom of the browser, address should be https://).
- All computers that hold personal information should have a password which complies with council security policy to move through before access is granted.
- Files containing personal/sensitive data should not be left unattended; there should be a secure password on the file and whenever possible the desktop should be locked.
- Files contained on 'data sticks' should have a password to access them (eg Excel or Word password) and should not be used as permanent storage unless locked and stored in the same way that paper records are archived.
- Should a person with access to the data leave the organisation, their access rights (on PCs etc) should immediately be removed.
- If a physical transfer of significant numbers of unencrypted electronic format be necessary, two persons should oversee the transfer at all times.



- A register of transfers should be taken at the departure and receiving end of the transfer, this register should not be overseen by those transferring the records.
- Any records within this scheme held or transferred to a location outside of a main location should be encrypted to 256bit level, independent of passwords on the files themselves.
- All records that hold sensitive data should be encrypted to 256bit level independently of passwords on the file.
- Records should be held only in a main location.

When Working With Customers Forms

- Registration forms should include a statement providing information on how and why the data will be stored, who the information may be shared with and who will be able to contact them via the information they have submitted. Notice of this will be then given once the customer begins to fill out the registration form.
- Notices will be placed on shared computers to remind customers that documents should not be saved onto the desktop and if so, the learners are doing it at their own risk.
- Only registers with a short statement, informing the customer that the information on the register sheet will be seen by others in the class, will be passed around for each customer to sign. Alternatively, registers should be taken only by the tutor so that no personal information regarding other customers can be obtained.

Procedures For Sub-contractors To Submit Data To CW&C

Sub-contractors must have passed the mandatory security sections of the procurement process including the completing of ICO checklists ensuring that they and their ICT systems comply with data security best practice.

Subcontractors should use an electronic system to complete data for their courses and learners. If using physical forms the following guidelines should be used.

- Use copies of the forms provided by CW&C on [the Skills and Employment web page](#) unless they have explicit permission to do otherwise.
- Forms completed by learners and tutors during delivery must be stored securely in accordance to the procedures outlined in this document for working with hard copy data.
- To transfer these forms to CW&C sub-contractors must scan the forms onto a local PC before transferring the scans to CW&C's [secure Cryptex system](#). The local scan files should then be deleted.



- No data concerning CW&C learners may be stored electronically on any subcontractor ICT system other than for the brief period while scanned files are uploaded to Cryptex. The only exception to this is if a sub-contractor is delivering other services to the same individual outside of their contract with CW&C.
- Hard copy forms will be collected by arrangement by CW&C staff.
- At the conclusion of a contract in the scenario where a sub-contractor does not gain a contract for a subsequent year all hard copy data will be collected by CW&C and the sub-contractor will be asked to sign a contract closure document confirming that they no longer hold any CW&C learner data.