Information Security Policy **September 2023-August 2024**	
AIM:	To provide clear direction to staff and others about expected codes of behaviour in relation to Information Security
NAMED STAFF/PERSONNEL WITH SPECIFIC RESPONSIBILITY FOR INFORMATION SECURITY	• **Lead** – Steve Egan • **Deputies** – Anita McGreevy • **Nominated Trustee** – Russell Hogarth
DISTRIBUTION:	• CWP staff, volunteers and learners • Service users • Website
DATE FOR IMPLEMENTATION:	1st September2023
DATE OF NEXT REVIEW:	31st August 2024
AUTHOR:	Steve Egan – CEO
APPROVED BY:	Bill Adams – Chair of Trustees

Introduction

This policy relates to all information held and used by CWP.

CWP holds significant amounts of personal and other information, both electronically and in hard copy, and has legal, contractual and operational reasons for keeping this safe and secure. This policy gives broad guidance on how to achieve this.

Information Security Policy

The purpose of this policy is to protect CWP information assets from all threats, whether internal or external, deliberate or accidental.

The policy covers physical security and encompasses all forms of information security such as data stored on computers, transmitted across networks, printed or written on paper, stored on CD/DVD's, USB drives or spoken in conversation or over the telephone.

The CWP CEO is directly responsible for implementing the Policy and for adherence by staff.

Information Security Guidelines

It is the responsibility of each CWP employee to adhere to this policy. The attached guidelines will be given to members of staff during their induction and they are expected to comply with them. Inappropriate usage and failure to follow these guidelines may lead to disciplinary action being taken under CWP Disciplinary Procedures.

Managing Records

The CEO or a named person delegated on his/her behalf should ensure that creation, detention, archiving or destructions of both manual and electronic records are in line with business and legal requirements.

CWP has a duty to hold records for specified amounts of time to meet administrative and legal needs. Legislation also places requirements on the retention of records. Certain records must be held for a minimum period (e.g. financial information), while others must only be held as long as needed (e.g. personal information).

CWP's retention schedule as outlined at the end of this policy provides the minimum period for meeting these requirements.

Records must not be destroyed before the retention periods expire. After the retention period has expired, non-essential records may be destroyed immediately; the request to destroy vital and important records must only be done after clearing with the CEO.

Any destruction of confidential records must be carried out in an appropriately secure manner.

Computer Security

Computers are increasingly subject to theft. As CWP delivery is reliant on computers such theft can cause very considerable disruption. There are a number of steps to minimise direct or consequential loss:

Make sure that original operating system software and application discs together with the relevant license are stored in a safe place so they can reload them onto a replacement computer, if necessary.

- Make sure recent data back-ups are kept in a safe place.
- All equipment is insured.
- All equipment is security marked.
- Get the police to check their building security.
- Ensure relevant computers are kept in areas of accommodation where access is controlled to a degree that gives reasonable assurance that unauthorised physical access cannot occur in the normal course of work.

Computer viruses

Appropriate anti-virus software is installed on computers and that the virus definition files are kept up to date.

Unauthorised access

To prevent unauthorised access computers a BIOS password at start up, a password-protected screensaver and secure network passwords will be set up.

Storage Media

Any data on a mobile storage media, e.g. DVD, USB memory stick or CD/DVD, inevitably exposes it to risks of damage or loss. Staff will be reminded to use an appropriate protective cover or container for the media and take care not to expose the media to theft or avoidable loss. USB sticks should also be password protected.

INFORMATION SECURITY GUIDELINES

Introduction

During an employees work with CWP staff will be processing and holding significant amounts of personal and other information both electronically and manually. CWP has legal, contractual and operational reasons to keep this information safe and secure.

The following guidelines are prepared to highlight good practice in information security and staff are expected to comply with them at all times. Failure to follow these guidelines may lead to disciplinary action being taken under CWP's Disciplinary Procedures

Confidential information

All through this paper the phrase 'confidential information' is used to mean information referring to individuals, partner organisations or other parties which should only be shared with the intended authorised personnel.

Oral Communications

Oral communications, referring to individuals or other restricted matters, represent perhaps the most significant practical risk to the security of information. The layouts of CWP centre may mean that oral communications can be easily overheard. Staff are expected to take care that confidential information is not overheard by unauthorised people, which may include other staff, trainees or visitors. Any discussion that involves or potentially involves confidential information must take place using a separate office or a meeting room to avoid this.

Staff should share confidential information only with authorised personnel both within and outside CWP.

Staff will be made aware that conversations outside the office, for example, on a train or other form of public transport, or in a pub or restaurant, are fraught with risk.

Manual data

Hardcopies of confidential information will be kept securely i.e. in a locked filing cabinet, ideally in a room that can itself be locked within the office.

In order to avoid loss in the event of fire, flooding etc, consideration will be given to duplicating hard copy information that is not also held on computers, keeping the duplicate in a separate, secure location in order to avoid loss

Hardcopy information which is confidential should not be left on an unattended desk in an open or unlocked office.

Generally, hardcopy information may be transferred by post. It is a criminal offence to open mail while it is in transit, so the use of the stamp ‘private and confidential’ should ensure that only the recipient or senior personnel within an organisation opens mail after it has been received.

Certain classes of hard copy information must be shredded before they are disposed of. These include:

- Personnel documentation referring to individuals;
- Any documentation referring to learners or volunteers;
- Internal financial information;
- Commercially sensitive information;
- Any documents that are designated as confidential by another organisation or individual.

Information held on computers.

Electronic data is usually stored on the hard drives of desktop or portable computers, DVD's/CD's, or memory sticks. These items can be stolen, destroyed or critically damaged by accident or intent as well as accessed by unauthorised persons.

To minimise risk a comprehensive and appropriate backup process will be in place to minimise potential loss of data.

If a computer is used for learners, volunteers or other semi-public purposes, no confidential information will be accessible on the drives of the computers.

Portable computers carry an obvious enhanced security risk. Their portability means that they can be easily lost and they can be the object of theft because of their size, cost and desirability. Regular data backups, at least monthly and all staff reminded to exercise due vigilance and care in the transport and storage of these items outside the centre.

Five key threats to computer files and preventative measures

In order to protect the data that is held on computer CWP will protect the files on computer(s) from various systemic or malicious threats. There are five key threats to digital data:

- Drive failure;
- Computer viruses, Spyware/Trojan Programs ;
- Unauthorised access;
- Drive loss or theft;
- Improperly managed disposal of redundant computers.

In order to avoid these threats anti-virus software will be installed on computers and virus definition files are kept up to date. Email users will ensure that anti-virus software is configured to scan all emails.

Prevention of unauthorised access and passwords

In order to prevent unauthorised access to computers:

- All computers have BIOS password protected start up, and network logon if appropriate;
- Where computers are left on and unattended for incidental periods during the working day, they will be protected by a password protected screen saver or by locking the PC;
- At the end of the working day computers will normally be shutdown and switched off;
- Where computers need to be kept on, it will be protected by a password-based screen saver;
- A comprehensive data back up process.

All passwords will be held by the CEO in a secure file and location.

Computer disposal

All drives will effectively wiped or reformatted prior to disposal.

Breach

In the event of a data breach CWP will inform relevant authorities within 72 hours, giving full details of the breach and proposals for mitigating its effects.

User Access

CWP will provide, on request, personal information we hold on staff, learners, and volunteers.

Privacy Notice

Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.
It applies to all current and former employees, workers and contractors.
Full information can be found in the sub Policy, Information Security-Privacy Notice

Monitoring and Guidance

Responsibility for monitoring and the implementation of this policy in operations, resides with the CEO.

DOCUMENT RETENTION PERIODS

Introduction

The following list shows the minimum number of years for which some CWP documents should be retained in order to meet organisational needs and the statutory requirements.

Document	Period of Retention	Comments
1.1. **Agreements and related correspondence**		
Major agreements of historical significance	Permanently	
Contracts with customers, Suppliers Rental/hire purchase agreements Indemnities and guarantees Other agreements/contracts	Six years after expiry or termination of the contract	Six years is generally the time limit within which proceedings founded on a contract may be brought If the contract is executed as a deed, the limitation period is twelve years Actions for latent damage may be brought up to fifteen years after the damage occurs
1.2. **Property**		
Deeds of title	Permanently or until property disposed of	
Leases	Fifteen years after expiry	
1.3. **Accounts**		
Company accounts	For a minimum of seven years from the date they are made.	Best practice suggests retaining company accounts for seven years from the year end Some accounting records will be required for tax purposes. Other funders may have similar requirements.

1.4. **Tax**		
Supporting documentation for tax returns: VAT	Six years	Note in general that where there is an enquiry into a tax return, records should be retained until the enquiry is complete
PAYE	For PAYE records not required to be sent to the Inland Revenue, not less than three years after the end of the tax year to which they relate	Note however that payroll records should be kept for five to six years
1.5. **Banking Records**		
Cheques, bills of exchange and other negotiable instruments, bank statements	Six years	
Instructions to banks	Six years after ceasing to be effective	
1.6. **Employee Records**		
Staff personal records	When employment ceases they should be retained for 6 months and then destroyed	.
Applications for jobs-where the candidate is unsuccessful	Six months after notifying the unsuccessful candidate	
Payrolls/wages	Six years from the year end	
Expense accounts	Six years	
Sickness records	Three years after the end of each tax year for Statutory Sick Pay purposes	
Accident books	Three years from the date of each entry	
Health and safety records	Three years	Personal injury actions must generally be commenced within three years of the injury. However, in some cases time

		periods may be substantially extended, check with HR Team.
1.7. **Insurance**		
Policies	Three years after lapse	
Employers liability certificate	40 years	
Claims correspondence	Three years after settlement	
Accident reports and relevant correspondence	Three years after settlement	
1.8. **Learner Records**		
Learner personal and activity	Six years	Experience tells us that we can get enquires from or about former learners.
Learner personal and activity records – core hardcopy record, including copies of qualification certificates	Six years	Experience tells us that we can get enquires from or about the qualifications gained by former learners.
Contract related learner records	A minimum of three years from the contract year in which the learner left our provision, but the minimum period may be greater by contract / funding agreement specification. For example, ESF related learner records have to be kept for a minimum of six years from the final settlement of the funding that supported the learner.	
1.9. **Volunteer records**		
Personal Files –	As employees	
1.10. **Disclosure Records**		
Disclosure information relating to employees and volunteers which is in a	Up to six months to allow for the consideration and resolution of any disputes	If, in very exceptional circumstances, it may be considered necessary to keep Disclosure information for

secure storage away from personnel or volunteer's file.	or complaints after which time the disclosure **MUST** be destroyed.	longer than six-months, we should consult the DBS about this and give full consideration to GDPR Protection and the Human Rights of an individual before doing so.
1.11. **ESF**		
All documents	* Specifically for current ESF project (2019-2021) document retention date is 31 December 2030.	At the point of the document retention date and before any ESF project documentation is destroyed, a check will be made on the gov.uk website to ensure it is safe to do so.

This policy will be reviewed on an Annual basis