



European Union
European
Social Fund



Information Security Policy -CCTV September 2021-August 2022	
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	<ul style="list-style-type: none"> • Lead – Steve Egan • Deputies – Anita McGreevy • Nominated Trustee – Holly Breakell
DISTRIBUTION:	<ul style="list-style-type: none"> • CWP staff, volunteers and learners • Service users • Website
DATE FOR IMPLEMENTATION:	1 st September 2021
DATE OF NEXT REVIEW:	31 st August 2022
AUTHOR:	Steve Egan – CEO
APPROVED BY:	Bill Adams – Chair of Trustees

Information Security Policy-CCTV

Introduction

This policy relates to all information held and used by CWP and specifically relates to the ESF contract 2019-2021.

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.

CWP is registered with Information Commissioner's Office under registration number **ZA088673**

The purpose

CWP is using CCTV system to ensure the safety of the centre users and as a security measure against theft and damage to CWP properties. CWP works with young people aged 13-19, whose behaviour can be challenging at times. Over the time we have witnessed damage to our premises, theft, aggressive, threatening behaviour, assault, false accusations and more. CCTV is part of our safeguarding policy. The cameras are situated in all main parts of the building:

- Reception
- Hair and Beauty Salon
- Hair & Beauty Training Room
- Editing Room
- Music Room
- Front entrance to the building
- Social Zone
- Child Care Area
- Production and Printing Area

CCTV cameras are sensor sensitive and start recording if any movement in the room is detected. The recording is then stored on the hard drive for a period of 12 days. After 12 days the recording is automatically erased. The hard drive is stored in a locked cabinet.

Notices advising CCTV is operating must be clearly displayed around the building. All centre users are made aware of CCTV during their induction.

Access to information

Access to CCTV footage is password protected. The footage can be accessed by authorised staff members following any incidents in the building. Any incident must then be recorded in the Issue Log stored on the shared area on Google Drive.

The access to information to anyone outside CWP can be granted by the CEO or other senior member of staff, authorised by the CEO only. The access can be granted for law enforcement purposes only.

Requests for CCTV footage should include relevant times and views from specific cameras only. Any footage can be transferred onto a recording device. This has to be recorded onto CCTV Record of Request with relevant details (name of the person authorising the release of the footage, date of the footage, person requesting the footage, the reason for the footage being requested).

Information Security Policy-CCTV

The footage can be provided to the police in order to provide an evidence of any activity that would be classed as a Police matter. This includes incidents inside and outside the building. When handing CCTV over to a third party CWP must make it clear that the responsibilities under Data Protection Act for the information that is being transferred will vest with the recipients of the information.

Complaints

Any complaints should be raised directly with CEO Steve Egan. Any complaints should be recorded and responded to within 10 working days.

This policy will be reviewed annually.