



Information Security Policy -E Safety September 2023 - August 2024	
AIM:	To provide clear direction to staff, learners and others about expected codes of behaviour in relation to Information Security and E Safety
NAMED STAFF/PERSONNEL WITH SPECIFIC RESPONSIBILITY FOR INFORMATION SECURITY	<ul style="list-style-type: none"> • Lead – Steve Egan • Deputies – Anita McGreevy • Nominated Trustee – Holly McClave
DISTRIBUTION:	<ul style="list-style-type: none"> • CWP staff, volunteers and learners • Service users • Website
DATE FOR IMPLEMENTATION:	1 st September 2023
DATE OF NEXT REVIEW:	31 st August 2024
AUTHOR:	Steve Egan – CEO
APPROVED BY:	Bill Adams – Chair of Trustees

Information Security Policy-E Safety

Introduction

Creativity Works Preston (CWP) works with the most vulnerable and challenging young people, the vast majority of whom have had little if any regular school attendance.

Our main priority is to offer an environment where young people feel at home and comfortable in the surroundings. Our aim is to engage young people, particularly at the start of their experience when rapport is at its lowest. It is our firm belief that were we to be restrictive in the 'fun things' we have to offer, many learners would not engage, resulting in disengagement and disenfranchisement.

Safeguarding young people at the centre is our absolute priority, reflected in our corporate values. We take every opportunity to encourage and support the welfare and development of the young people in our care, for example, informal partnerships with neighbouring Colleges and feeder schools to review and ensure consistency.

Background

CWP has a Safeguarding policy, developed with advice from a Local Safeguarding Children Board. This e-safety policy is designed to complement this.

The Internet and related technologies are powerful tools which present new prospects for communication and collaboration. Education and training are embracing these new technologies as they bring with them fresh opportunities for both staff and learners.

“To use these technologies effectively requires an awareness of the benefits and risks to the development of new skills and an understanding of their appropriate and effective use both inside and outside of the classroom” DfES strategy (2005)

The Green Paper, Every Child Matter, the provisions of the Children Act (2004) and Working Together to Safeguard Children (2010) sets out how organisations and individuals should work together to safeguard and promote the welfare of children and young people.

All the 5 outcomes apply equally to the virtual worlds that children and young people will encounter, whenever they use ICT in its various forms. For example, we know that the Internet has been used for grooming children and young people with the aim of exploiting them sexually and we know that ICT can offer new weapons for bullies who may torment victims via websites or text messages. We also know that children and young people have been exposed to inappropriate content when online which can sometimes lead to their involvement in crime and anti-social behaviour.

ICT in the 21st century has an all-encompassing role within the lives of young people. Current and emerging technologies include:

- World wide web
- E-mail
- Instant messaging
- Blogs
- Podcasting
- Social networking sites, e.g., Facebook, Twitter, Instagram, Snap Chat, Tik Tok

CWP Information Security Policy – E Safety

September 2023

Owner: Steve Egan

Review Date: September 2024

Information Security Policy-E Safety

- Video broadcasting sites
- Gaming sites
- Music download sites
- Mobile phones with cameras/video functionality
- Smart phones with e-mail/web functionality
- On-line learning resources

CWP complies with the OFSTED Safeguarding Guidance and has a staff behaviour policy which includes 'do's and 'don't's and references staff/student relationships and communications. We also recognise and support DfE recognised expert, Childnet

'The internet is a brilliant place to connect with others, to be creative and to discover new things.

In terms of an e-safety policy, all staff at CWP are familiar with the policy, including:

- Safe use of e-mail
- Safe use of the Internet, including use of Internet based communications services, such as instant messaging and social networks, e.g., CWP Facebook page
- Safe use of digital images and digital technologies such as mobile phones and digital cameras
- Publication of learner information, photos and use of websites
- E-bullying/cyber bullying procedures
- The role of staff in providing e-safety education for students

Policy

CWP uses Facebook in order to interact whilst at the centre but are also aware of the potential risks involved. We do not feel it is appropriate to deny learners access to the Internet and we have no plans to introduce controls. Whilst we accept there are risks, like everything in life, we believe the answer is education not prohibition.

CWP believe the young people in their care can make informed choices about responsible use of social media and to panic and simply deny access to any social media sites may have a negative effect on young people continuing to attend the centre, in addition to the undoubted benefits the Internet has. To ensure that learners are not compromised by this policy, we have introduced the following changes:

Improved Induction:

Greater emphasis is placed on E Safety as part of the induction process. Whilst the Induction Handbook already contains sections on appropriate use of the Internet, we have added a section on e safety and the issues of cyber bullying and grooming. Learners are given an in-depth explanation as to why that is our policy and should be able to recall what safe and responsible online behaviour means and how to respond to issues. We also make our young people aware of the consequences around infringing our E-safety policy.

CWP Information Security Policy – E Safety

September 2023

Owner: Steve Egan

Review Date: September 2024

Information Security Policy-E Safety

Introduced a designated Internet Safety Co-ordinator (ISCO) Peter Hall. The ISCO will support staff in being updated/refreshed around e-safety matters at least annually or more regularly if practice suggests this is necessary.

Access training for the ISCO to ensure he/she is the onsite expert and able to support staff if issues arise.

Every PC will have a Screen saver-with key messages about E Safety-Don't talk to strangers-don't post offensive messages-Surf and be safe and posters displayed around the building.

Have the facility to be able to monitor the Facebook use of our young people if necessary and block sites if we feel this may be an appropriate course of action.

Introduced a proxy server that filters and blocks inappropriate websites.

E safety and social networking is addressed through project activity. Every TV show has a News Feature on E Safety and the dangers of inappropriate use. Every learner will produce at least one news feature that will look at a current issue and how to deal with the dangers.

We will also consider how e-safety complaints are handled and adopt a policy of responding should an e-safety incident be reported. A log of e-safety incidents with resulting outcomes and any follow up will also be available for inspection. Young people are given information on external sources of advice and support should they have e-safety issues.

We have adjusted our anti-bullying policy to take account of cyber bullying and have posters and reminders about safer surfing around the centre.

UpToDate information can be found at

<https://www.gov.uk/government/publications/coronavirus-covid-19-keeping-children-safe-online/coronavirus-covid-19-support-for-parents-and-carers-to-keep-children-safe-online>

This policy will be reviewed annually.