European Union
European
Social Fund

Education & Skills
Funding Agency

Online Safety Policy

1. Introduction

Skills People Group consists of the following companies.

- *Construction Skills People*
- *C&G Assessments and Training Ltd*
- *Training Futures UK Ltd*

The company is committed to its ongoing duty of care to safeguard its stakeholders including, staff, learners, visitors and self-employed partners. The company recognise in their use of technology to establish mechanisms which identify, intervene in, and escalate any incident where appropriate.

The use of technology has become a significant component of many safeguarding issues such as: exploitation; radicalisation; sexual predation; technology often provides the platform that facilitates harm. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- ***Content:*** *being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views;*
- ***Contact:*** *being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults;*
- ***Conduct****: personal online behaviour that increases the likelihood of, or causes harm; for example, making, sending and receiving explicit images or online bullying*.

2. Purpose

The purpose of this policy is to ensure that all its stakeholders including, staff, learners, visitors and self-employed partners achieve their full potential safely in an environment free from discrimination.

3. Scope

This policy applies to all stakeholders including, staff, learners, visitors and self-employed partners conducting onsite and offsite activities regardless of position, role and responsibilities.

4. Online Safety

The company recognises that online encompasses not only the internet but any type of electronic communication, such as mobile phones and devices with wireless technology. These new technologies are enhancing communication and the sharing of information, which inevitably challenge the definitions and boundaries of the learning and or working environment.

The importance of online safety includes, but is not limited to:

- **Cyberbullying** is when someone uses technology (such as the internet or a mobile phone) to bully others. - Cyberbullying can happen in a number of different ways including receiving nasty messages or emails, being the target of a hate group on a social networking site, having embarrassing photos and videos shared publicly online or being excluded from group conversations. Content can be circulated very quickly and anonymously on the internet and there are often lots of bystanders which can make the experience more traumatic and harder to combat.

- **Online grooming** is the process by which an adult will approach a child online, with the intention of developing a relationship with that child, to be able to meet them in person and intentionally cause harm. The motivation behind this is most likely to be sexual. However, not all adults who seek to groom children online have an intention of meeting up with the child. Instead their intention may be to coerce the child into taking sexually explicit photos or videos and to send these to the adult. Alternatively, their motivation could be financial gain from the child or their family.

- **Online sexual harassment** is defined as unwanted sexual conduct on any digital platform. It includes a wide range of behaviours that use technology to share digital content such as images, videos, posts, messages, pages etc. on a variety of different platforms (private or public). When referring to sexual harassment we mean 'unwanted conduct of a sexual nature' that can occur online and offline. This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include:
    - *Non-consensual sharing of sexual images and videos;*
    - *Sexualised online bullying;*
    - *Unwanted sexual comments and messages, including, on social media;*
    - *Sexual exploitation; coercion and threats*

- **Sexting** - the term **'sexting'** describes the use of technology to share personal sexual content. It's a word-mix of sex and texting. Young people tend not to use this term but may use other nicknames such as 'nudes', 'nude selfies' or imply these through the context of the message.

- **Identify theft**: your name, address and date of birth provide enough information to create another 'you'. An identity thief can use a number of methods to find out your personal information and will then use it to open bank accounts, take out credit cards and apply for state benefits in your name. The main component of "card ID theft" is data obtained by fraudsters through methods including phishing emails, scam texts and the theft of mail from external mail boxes and multi-occupancy buildings.

- **Online gambling** as with many other online activities – carries the risk of criminal activity. However, there are also other specific associated risks, such as payouts not being fair and open, access by children and use by vulnerable people. Gambling can also be addictive, and you need to know when to stop.

- **Radicalisation** refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur online through exposure to and engagement with violent ideological propaganda, or offline through extremist networks. Radicalisation makes those at risk more likely to support terrorism and violent acts of extremism, and possibly even commit such criminal acts themselves. Social media sites, like Facebook, Ask FM and Twitter, can be used by extremists looking to identify, target and contact young people. It's easy to pretend to be someone else on the internet, so children can sometimes end up having conversations with people whose real identities they may not know, and who may encourage them to embrace extreme views and beliefs.

- **Online gaming** is hugely popular with children and young people and there are many ways for users to connect and play games online. Online safety advice is directly applicable to the gaming environment because of the risks that are present. It is essential that children are aware of these issues and are given the skills and knowledge to help manage and reduce these risks, with the help of those around them.

- **Staying safe and responsible:** Illegal file-sharing programmes and websites pose greater risks to your computer or mobile phone than legitimate sites. Users often unwittingly download viruses or spyware and can inadvertently share personal computer files and information. Some files are purposely misnamed on file-sharing and peer-to-peer networks to trick people into downloading them.

- **Downloading** music, film and TV on the internet - what you should know**:** Copyright law applies to downloading, sharing and streaming just as in the world of physical CDs and DVDs. If you make music, film or TV content available to others on a file-sharing network, download from an illegal site, or sell copies without the permission of those who own the copyright, then you are breaking the law and could face serious penalties.

- **Social networking** sites such as Instagram and Snapchat are very popular with young people, even those who are of primary age. These types of sites allow individuals to be incredibly creative online, keep in touch with their friends and family, as well as share photos and videos. It's important to familiarise yourself with social networking services. Content which is uploaded online can be copied, altered and reposted by anyone and it is very difficult to 'take back' what may be later regretted.

- Like social networking, **emails and text messaging** follow many of the same rules as social networking. Sometimes a message can be read in the wrong way and can upset or hurt someone's feelings. Emails must be addressed and sent carefully. Users must take extreme care when typing in addresses, particularly when email address auto-complete features are enabled; using the "reply all" function; or using distribution lists to avoid inadvertent information disclosure to an unintended recipient. To ensure data is kept secure, attachments containing 'personal data' must be encrypted or password protected as a minimum requirement. The encryption key or password must be communicated using a different method of communication i.e. disclose the password over the telephone or by text.

- **Spam emails** - one of the major dangers to personal information that internet users face on a day-to-day basis are phishing emails. These are emails which are designed to look as though they come from a legitimate source, such as your bank, building society or PayPal account. They will often talk about a security breach or a transaction which you do not know about, and they may give you a link to log in with, so that you can verify the transaction or confirm your details. Clicking on one of these links is likely to take you to a website that looks just like the site that you are expecting to visit, but it is one which is designed to harvest your account information. Look carefully at all emails before clicking on links enclosed within them. Poor spelling and grammar, and an unfamiliar writing style are all tell-tale signs of a phishing email, however more sophisticated scams look near perfect. Other tell-tale signs include an unfamiliar email address or site URL. You should be particularly vigilant about domain suffixes (.com, .co.uk, .net etc). Although most of the URL may look the same as the site that you are expecting, it may be a fake site if the suffix is different.

- **Importance of using strong passwords** – if you have a large number of online accounts, do not choose the same password for every account. This could mean that if a hacker finds your log-in details for a minor account (such as a chat forum), they may then be able to use exactly the same password to log in to some of your more important accounts. In addition to using different passwords, you should also make sure that you are using a strong password. A strong password includes uppercase and lowercase letters, as well as numbers. Make sure that your password is not on any list of common passwords (these include "password" and "qwerty"), and do not use a word which can be guessed easily by

someone who knows about your life, such as the name of your cat or the name of your favourite football team. If your account provider allows it, you can also strengthen your password by adding a symbol, such as a #.

5. Implementation

- The curriculum enables learners to build on knowledge of: Safeguarding including: Prevent, **Online Safety**, Equality and Diversity, British Values during induction and all the aforementioned including Equality and Diversity during learning sessions

- Monthly 'Hot Topics' are distributed via internal communications to raise awareness and promote discussion around the wider safeguarding agenda including areas such as: British Values, Radicalisation, Mental health issues, positive relationships, **Staying Safe Online,** Health and Safety, Equality and Diversity and Health and Wellbeing.

- Safeguarding, Equality and Diversity, **Data Security** and Health and Safety remain a fixed agenda item at all meetings.

- No company-owned or company-provided computer systems may be knowingly used for activities that are considered illegal under local, national, or international law.

- Internet sites are blocked which have harmful content via the Cyberoams

- In order to stay safe **online** all staff are required to read and follow the relevant IT policies.

- Staff are required to complete staying safe **online** training during their induction.

- Visitors are granted access to a guest internet site only.

- Action may be taken to intervene, where appropriate, in online incidents that take place beyond the company.

6. Reporting an Online Safety Concern (Safeguarding, Prevent and online safety)

If a member of staff or self-employed partner is unsure if their concern is safeguarding, they are required to seek advice from a member of the safeguarding team.

Help and advice between Monday-Friday 8am – 5pm contact a member of the Safeguarding team

Email safeguarding@skillspeoplegroup.com

Concerns about a child's welfare must be reported immediately to the designated safeguarding lead or deputy lead. **Refer to the reporting procedure within the Safeguarding and Prevent Policy*.

Designated Safeguarding Lead: (Strategic Lead) Sacha McCarthy: Director of Quality & Operations Tel: 01246 589 444 Mobile: 07976 744655
Deputy Designated Safeguarding Lead: Perry Adams, HR Advisor Tel: 01246 589 501 Mobile: 07860 917688
Safeguarding Officer: Alan Briggs, South Yorkshire Skills Academy Manager Tel: 01246 589 444 Mobile: 07908598732
Safeguarding Officer: Kelly Kirk, Nottingham Skills Academy Manager Tel: 01246 589 444 Mobile: 07495 681473

10. External Agencies: Information, Advice and Guidance

- **Reporting abuse**: contact the local police https://www.police.uk/ if you think a crime has been committed.
- **Help for a gambling problem** https://www.nhs.uk/live-well/healthy-body/gambling-addiction/
- **Helping children stay safe online** https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
- **Grooming** the NCA's CEOP Command (formerly the Child Exploitation and Online Protection Centre) works with child protection partners across the UK and overseas to identify the main threats to children and coordinates activity against these threats to bring offenders to account. https://www.ceop.police.uk/safety-centre/
- **Cyberbullying:** ChildLine: NSPCC has set up this website especially designed for children and young people who would like free confidential information on issues such as cyberbullying or abuse. https://www.childline.org.uk/
- **Fraud and Financial Scams:** Action fraud is a national public facing organisation to help tackle fraud in UK. Action Fraud is supported by the National Fraud Authority. https://www.actionfraud.police.uk/ Tel: 0300 123 2040
- **Fraud and Financial Scams:** Bank Safe Online is the UK banking industry's initiative to help online banking customers stay safe online. This site is run by the UK Payments Administration on behalf of its member banks.
-

- https://www.financialfraudaction.org.uk/consumer/advice/protect-your-onlinemobile-banking/
- Thinkuknow **Gaming:** provides safety advice for online, **chatroom** safety https://www.thinkuknow.co.uk/
- **Gaming:** The Association for UK Interactive Entertainment (UKIE) is the UK's leading videogames trade body. https://ukie.org.uk/
- **Online Terrorism** The government has developed a reporting mechanism for members of the public to refer what they believe to be unlawful terrorist material directly to the police for its removal. https://www.gov.uk/report-terrorism
- **Internet Safety**: UK Safer Internet Centre has published extensive guidance on how to stay safe on the internet. They have advice for children, parents and teachers. https://www.saferinternet.org.uk/
- **Safeguarding Children** - Sheffield Safeguarding Hub Office hours are from 8.45am to 5.15pm (Monday to Thursday) and 8.45am to 4.45pm (Friday) at all other times including Bank Holidays, calls will be responded to by the Emergency Duty Service **01142 734450** Email: sscb@sheffield.gov.uk https://www.safeguardingsheffieldchildren.org/sscb
- **Personal safety:** contact the Police 999 or 101
- **Health and Wellbeing** contact your out of hours Doctors or call the Hospital on 111
- **Radicalisation** https://www.internetmatters.org/issues/radicalisation/
- https://safe.met.police.uk/internet_safety/other_help_and_advice.html
- https://www.iwf.org.uk/
- **Hate Crime:** True Vision gives you information about hate crime or incidents and how to report it. http://www.report-it.org.uk/home
- **Hate Crime:** Quilliam is the world's first counter-extremism think tank set up to address the unique challenges of citizenship, identity, and belonging in a globalised world. https://www.quilliaminternational.com/
- **Mobile Phone Issues:** The British Board of Film Classification (BBFC) provides the independent framework that underpins the Mobile Operators' code of practice for the self-regulation of content on mobile. The Classification Framework defines content that is unsuitable for customers under the age of 18 and is based on the BBFC's Classification Guidelines for film and video. https://bbfc.co.uk/what-classification/mobile-content
- **Mobile Phone Issues:** The Mobile Broadband Group (MBG) brings together all the UK mobile network operators (O2, Vodafone, Three and EE) to work across a range of self-regulatory initiatives and public policy issues in the mobile sector. http://www.mobilebroadbandgroup.com/
- **Copyright Issues:** Federation Against Copyright Theft (FACT): FACT's primary purpose is to protect the United Kingdom's film and broadcasting industry against counterfeiting, copyright and trademark infringements. https://www.fact-uk.org.uk/

8. Incident Reporting

Data Protection incidents must be reported immediately to the Data Protection Officer.
The Data Protection Officer is Steve Cressey on 07773322079 / 01246 589444.

9. Enforcement

Violations to this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

The company will take all necessary steps to report and prosecute any violations of this policy.

11. Applicability of Other Policies

This policy should be read in conjunction with:

- *Safeguarding and Prevent Policy*
- *Password Policy*
- *Email Policy*
- *Acceptable Use Policy*
- *Mobile Device Policy*
- *General Data Protection Policy*
- *Removable Media Policy*
- *Physical Security Policy*
- *Modern Day Slavery Policy*
- *Incident Response Policy*

Document Control

Date of change	Version	Overview of amendment	Amended by / Job title	Approved by	Approval date
14-10-19	1	Policy created	Julie Lawton (Quality Manager)	Amanda Warham (Operations Director)	18/10/19
20-11-19	2	**Section 5 - Implementation** • **Page 5** – the following has been added to the implementation list. *Action may be taken to intervene, where appropriate, in online incidents that take place beyond the provider.* **Section 6 -Reporting safeguarding concerns** • **Page 6 –** Addition to the Safeguarding team. *Stuart Brown has been added as a Safeguarding Officer*	**Julie Lawton (Quality Manager)**	Amanda Wareham (Director) and SMT	Pending approval
17.09.20	3	**Section 6 – Reporting** Safeguarding Concerns • Page 6 – removal of Amanda Wareham and Julie Lawton, added Sacha McCarthy as Strategic Lead, Kelly Kirk and Chris Clark as Safeguarding officers. **Section 8 – Reporting Incidents** • Page 8 – Removal of Amanda Wareham as the data protection officer and added Sacha McCarthy as the replacement	Sacha McCarthy (Group Head of Quality & Performance)	Sacha McCarthy (Group Head of Quality & Performance) and SMT	21.09.20
14.09.21	4	**Section 6 – Reporting Safeguarding Concerns** • Page 6 – Removal of Sarah Booth, Chris Clark and Stuart Brown as Safeguarding Officers and addition of Alan Briggs as Safeguarding Officer. **Section 8 – Reporting Incidents** • Page 7 – Removal of Sacha McCarthy as DPO and addition of Steve Cressey as DPO.	Brendan Knowles Head of Quality & Performance	Brendan Knowles Head of Quality & Performance	14.09.21