

SG Policy appendix 5

Online & eSafety Policy

Introduction

Reflections Training recognises the benefits and opportunities which new technologies offer to teaching and learning. We encourage and embrace the use of technology in order to enhance skills and promote achievement. However, the accessible and global nature of the internet and the variety of technologies available, mean that we are aware of potential risks and challenges associated with such use. Our approach is to ensure learners are safeguarded from potentially harmful and inappropriate online material through the implementation of safeguards and to support staff and learners to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training, and guidance and implementation of our associated policies. To further our duty to safeguard learners we will so far as reasonably practical do all that we can to make our learners and staff stay safe online and to satisfy our wider duty of care. This Online safety policy should be read in conjunction with other relevant Academy policies.

The following Directors by signing this document show their support to successfully achieve Reflections Training Academy's Online & eSafety & Safeguarding Goals.



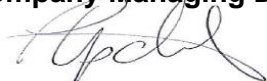
Senior Manager Divisional Prevent / Safeguarding (DSL)

Reflections Training Academy

This policy was considered and adopted by the following Directors:



Clare Barrett
Company Managing Director



Phil Davis
Director of Bristol Training Academy



Lucy Agnew
Divisional Director of Training



Kate Sperring
Director of Next Level Training

Policy Owner	Director sign off	Details of update	Date of Update	Version number
Jason Timms	Lucy Agnew	Policy review & Update	28/11/2019	13
Jason Timms	Lucy Agnew	Policy rename & rewrite	29/06/20	14
Jason Timms	Lucy Agnew	Policy review & Update	21/04/21	15
Jason Timms	Lucy Agnew	Policy review & KCSiE 2021 Update	17/09/21	16
Jason Timms	Lucy Agnew	Policy review & KCSiE 2022 Update	16/08/22	17
Jason Timms	Lucy Agnew	Policy review & KCSiE 2023 Update	25/08/23	18

Next review date: ~~Ed August 2024~~ August 2024

What is Online Safety?

Online safety defined as being safe from risks to personal safety and wellbeing when using all fixed and mobile devices that allow access to the internet, as well as those that are used to communicate electronically.

It means ensuring that children and young people are protected from harm, and supported to achieve the maximum benefit from new and developing technologies without risk to themselves or others. This includes personal computers, laptops, mobile phones and games consoles such as Xbox, PlayStation and Nintendo Switch

The aim of promoting online safety is to protect young people from the adverse consequences of access or use of electronic media, including bullying, inappropriate sexualised behaviour or exploitation. Many of these risks reflect situations in the non-digital off-line world. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build Learners' resilience to the risks to which they may be exposed, so that they have the skills and confidence to face and address these risks.

Safeguarding against these risks is not just an ICT responsibility; it is everyone's responsibility and is considered as part of the overall arrangements in place that safeguard and promote the welfare of all members of the Reflections Training community, particularly those that are vulnerable.

The term 'safeguard' is defined for the purposes of this document in relation to online safety as the process of limiting risks to learners when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and inspection.

Online safety policy statement

The aim of this policy is to ensure staff and learners, use Reflections Training internet and Information and Communication Technology (ICT) equipment safely and appropriately, ensuring the best possible outcomes for our learners.

The main areas of risk for Reflections Training Academy as a learning provider can be summarised as follows:

Content:

- exposure to illegal, inappropriate or harmful material, including online pornography, online gambling, drug paraphernalia, harmful online challenges and hoaxes
- Extreme lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Exposure to socially unacceptable material, such as that inciting violence, misogyny, racism, anti-Semitism, hate, extremist views or intolerance
- Exposure to fake news and inaccurate or misleading information and how to check the authenticity and accuracy of online content.
- Exposure of minors to inappropriate commercial advertising or commercial and financial scams

Contact:

- being subjected to harmful online interaction with other users, e.g. peer on peer pressure
- commercial advertising and adults posing as children or young adults with intention to groom or exploit them for sexual, criminal, financial or other purposes
- child sexual exploitation
- cyber-bullying in all forms
- extremism and radicalisation
- identity theft, online fraud, Phishing.

https://reflectionstrainingacademy-my.sharepoint.com/personal/lucy_reflectionstraining_co_uk/Documents/Lucy/Policies and Procedures 2024/Safeguarding/SG Policy Appendix 5 - Online Safety policy - Version 18.docx

- hacking *Educate to Innovate*

Conduct:

- personal online behaviour that increases the likelihood of, or causes, harm
- privacy issues, including disclosure of personal information or and sharing passwords.
- digital footprint and online reputation inclusive of Equality & Diversity responsibilities, defamation of others
- health and well-being - the amount of time spent online (socialising, watching video or gaming)
- making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi nudes and/or pornography, sharing other explicit images)
- copyright and plagiarism (no thought or consideration for intellectual property and ownership – such as music and film).

Commerce

- Online gambling and gaming
- Online fraudulent financial activity and scams
- Password and account hacking
- Spam email and messages

Scope

Reflections Training Academy will deal with such incidents within this policy under its Safeguarding, behaviour and anti-bullying policies, and will, where known, where appropriate inform parents/carers and employer of incidents of inappropriate online safety behaviour that take place inside or outside of Reflections Training Academy

This policy has been created in line with the statutory guidance document **Keeping Children Safe in Education, 2023**.

Communication

The online safety policy will be communicated to staff and learners in the following ways:

- policy to be uploaded to MyConcern and all staff are required to confirm they have read & understood;
- policy to be part of Safeguarding induction pack for new staff;
- Copy available via the Reflections Training Academy / Next level Websites;
- Acceptable use agreements to be issued to learners during the induction period
- acceptable use agreements to be held in learner personnel files;
- All learners and tutors will be provided with online safety training.

Handling complaints

Reflections Training Academy will take all reasonable precautions to ensure online safety as detailed within the ICT & eSafety Arrangements inclusive of firewalls, content filtering and Lanschool monitoring software. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a Reflections Training Academy computer or mobile device.

Staff and learners are given information about actions to be taken in the event of a complaint or breach of this policy

These include:

- Interview with DSL and /or Academy Director

- If applicable informing parents/carers or apprenticeship employer
- Referral to Local Authority and/or police

The DSL acts as the first point of contact for any online safety complaint.

Complaints of cyberbullying are dealt with in accordance with our Expectations & Behaviours Policy; Complaints and/or allegations related to Safeguarding are dealt with in accordance with the Reflections Training Academy and Local Authority Safeguarding procedures:

- Complaints about Remote Online sessions must be made within 5 days of the session being made.
- All complaints will be dealt with in accordance with our Complaints Policy.

Review and Monitoring

The online safety policy is referenced from within other Reflections Training Academy policies:

- ICT Safety Arrangements,
- Safeguarding policy,
- Anti-Bullying policy,
- Expectations & Behaviours policy.

The online safety policy will be reviewed annually or when any significant changes occur regarding the use of technologies within Reflections Training Academy

All amendments to the Reflections Training Academy Online Safety Policy will be communicated to all members of staff.

Remote online sessions will be monitored in line with the Academy IQA and observation policy.

Online Safety Lead – are responsible for ensuring that

Each academy DSL will have responsibility for Online Safety. They will develop and maintain an online safety culture within Reflections Training Academy. The DSL's will cover for each other's absence.

The responsibilities of this role are to:

- a. Develop an online safety culture at Reflections Training Academy
- b. Be the named point of contact on all online safety issues
- c. Ensure online safety is included as part of the induction procedures, and all staff and volunteers receive a copy of this policy, the **Acceptable Use Policy**, and return it signed and dated
- d. Monitor online safety, such as:
 1. ensuring the technology infrastructure provides a safe and secure environment for learners and staff
 2. Maintaining an online safety incident log on MyConcern, to record user concerns and incidents
- e. Reporting on online safety issues to the Directors
- f. Ensure that all learners, staff, and management members know what to do if they are concerned about an online safety issue
- g. Keep abreast of developing online safety issues via attendance at relevant training sessions, conferences or seminars, and recommended websites such as:
 - a. <http://www.saferinternet.org.uk/>
 - b. <http://www.thinkuknow.co.uk>
 - c. <http://www.ceop.police.uk>
 - d. <https://swgfl.org.uk/>

- h. Ensure that online safety is embedded within continuing professional development (CPD) for staff and volunteers, and co-ordinate training as appropriate
- i. Ensure that online safety is embedded across all activities as appropriate
- j. Ensure that online safety is promoted to learners, whilst at Reflections Training Academy

- k. Review and update online safety policies and procedures on a regular basis and after an incident.

- l. Ensuring Biannual testing of the in-house learner accessible IT systems and servers is carried out

Technical support staff are responsible for ensuring that:

The IT technical infrastructure is secure; this will include at a minimum:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows (or other operating systems) updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solutions such as Internet filtering/monitoring are operating correctly.
- Filtering levels are applied appropriately and accordingly and that categories of use are discussed and agreed with the safeguarding team and senior management team.
- Continue to research and implement new technologies which will improve IT security and safeguarding measures.
- Passwords are applied to all users and correctly used in line with company policy.
- Highlight and report in a timely manner any e-safety concern or system alert to the designated safeguarding leads via MyConcern.

All Staff

Staff are to ensure that:

- Any e-safety incident is reported to the DSL (and a safeguarding concern is made), or in his/her absence to a member of the senior management team.
- Correct password usage and control is enforced and any deviation is reported.
- Ensure that all users of technologies adhere to the standard of behaviour as set out in the ICT Acceptable Use Agreement and Staff Code of Conduct.
- Apply appropriate security to devices when left unattended (e.g. lock screen)

The curriculum

Learner online safety

Reflections Training Academy has clear, progressive online safety sessions embedded as part of the Study and Apprenticeship programmes. This covers a range of skills and behaviours appropriate to the learners' age and experience, including:

- How to develop a range of strategies to evaluate and verify the information before accepting its accuracy
- How to be aware that the author of a website, blog or post may have a particular bias or purpose, and to develop skills to recognise what that may be;
- How to demonstrate polite and acceptable behaviour when using software services in an online environment
- How to understand why they must not upload pictures or videos of others without their permission
- How to know not to download any files – such as video or music files - without permission from the copyright holder;
- How to have strategies for dealing with receipt of inappropriate material;

- How to understand why and how some people will 'groom' young people for criminal, anti-social or sexual purposes;
- How to understand the impact of cyberbullying, sharing of nude and semi-nude images and trolling, and know how to seek help if they are affected by any form of online bullying.
- How to know how to report any abuse and how to seek help if they experience problems when using internet-connected technologies, i.e. parent or carer, tutor or trusted staff member, or an organisation such the 'Click CEOP' button.
- Reminding learners about their responsibilities through the **Acceptable Use Agreement**, which every learner is inducted to and signs

- Ensuring staff will model safe and responsible behaviour in their own use of technology during sessions
- Ensuring that when copying content from the web, staff and learners understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge the copyright and intellectual property rights;
- Ensuring all learners complete the ETF 'Side by Side' Staying Safe Online module & assessment

Staff Training

Reflections Training Academy

- ensures staff know how to send or receive sensitive and personal data, and understand the requirement to protect data where the sensitivity of that data requires data protection
- makes online safety training available to staff
- provides, as part of the induction process, all new staff with information and guidance on the online safety policy, ICT & eSafety Policy and Reflections Training Academy's Acceptable Use Policies.

Parent awareness

Reflections Training Academy:

- Provides advice and guidance for parents, including:
 - Information on the website including recommended support and information sites
 - Signed parental agreement for online interviews and training sessions for all learners aged under 18

Use of ICT equipment

Where learners have access to browse the internet, staff must be vigilant in monitoring the content of the websites the learner's visit

Staff who use the Reflections Training Academy ICT and communications systems:

- a. must sign and abide by Reflections Training Academy **Acceptable Use Policy**
- b. must use the systems responsibly and keep them safe
- c. must maintain safe professional boundaries. This includes not giving their personal email address to learners or befriending learners on social network sites, such as Facebook or Instagram as detailed within the staff code of conduct
- d. will have clearly defined access rights to Reflections Training Academy ICT systems.
- e. must treat as confidential any passwords provided to allow access to ICT equipment or systems and not share under any circumstances
- f. must ensure the integrity of passwords. Network user account passwords should be strong (mixture of letters, number and characters) and be changed periodically, If a

<https://reflectionstrainingacademy->

[my.sharepoint.com/personal/lucy_reflectionstraining_co_uk/Documents/Lucy/Policies and Procedures 2024/Safeguarding/SG Policy Appendix 5 - Online Safety policy - Version 18.docx](https://my.sharepoint.com/personal/lucy_reflectionstraining_co_uk/Documents/Lucy/Policies%20and%20Procedures%202024/Safeguarding/SG%20Policy%20Appendix%205%20-%20Online%20Safety%20policy%20-%20Version%2018.docx)

password is compromised, it must be changed as soon as possible and no longer than within 24 hours;

- g. must not install software on the Reflections Training Academy equipment, including apps, freeware and shareware without the express permission of the senior management team
- h. must not use personal devices (e.g. USB memory sticks) to upload or download material onto Reflections Training Academy network or website, or any ICT device
- i. Any use of cloud storage systems (e.g. Dropbox, Google Drive, etc.) will need to be approved by an academy Director.
- j. Must comply with any ICT security procedures governing the use of systems in Reflections Training Academy, including anti-virus measures and device security
- k. Must report known breaches of this policy, including any inappropriate images, messages or other material which may be discovered on Reflections Training Academy ICT systems
- l. Must ensure that the systems are used in compliance with this online safety policy
- m. Will be provided with online safety training.
- n. Understand that system use, including but not limited to internet usage and system logs may be monitored.

Online safety and use of digital devices

At all times, staff, parents, and learners, will treat others with respect and will not undertake any actions that may bring Reflections Training Academy into disrepute.

Mobile phones, tablets and other digital devices can present several problems when not used appropriately.

- a. Mobile/smartphones, tablets and other personal devices can allow wireless and 3/4/5G internet access via alternative ISPs, and thereby bypass the Reflections Training Academy security settings and filtering;
- b. Mobile/smartphones with integrated cameras could lead to safeguarding, bullying and data protection issues, with regard to inappropriate capture, use or distribution of images of learners or staff.

Equipment

Reflections Training Academy is responsible for ensuring that the network infrastructure, computer equipment and internet provision is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

All computer equipment is installed professionally and meets current health and safety standards. Equipment is maintained to ensure health and safety standards are followed.

Internet access and Filtering & Monitoring

Reflections Training Academy Internet Service Provider (ISP) is BT.

Whilst considering our responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, Reflections Training Academy ensure that we do all that we reasonably can to limit children's exposure when using Academy IT systems. We use content filtering based on the Internet Watch Foundation (www.iwf.org.uk) model via GobaView, a service that is activated on the gateway router to capture all users of the internet facility that meets or exceeds the DfE Filtering & Monitoring Standards on all in-house learner accessible IT systems which are in place for the safety of all of our learners. This monitors, flags, and blocks access to websites that are blacklisted or considered to be dangerous, harmful or contain inappropriate content.

<https://reflectionstrainingacademy->

[my.sharepoint.com/personal/lucy_reflectionstraining_co_uk/Documents/Lucy/Policies and Procedures 2024/Safeguarding/SG Policy Appendix 5 - Online Safety policy - Version 18.docx](https://my.sharepoint.com/personal/lucy_reflectionstraining_co_uk/Documents/Lucy/Policies%20and%20Procedures%202024/Safeguarding/SG%20Policy%20Appendix%205%20-%20Online%20Safety%20policy%20-%20Version%2018.docx)

Lanschool monitoring software is in place on learner servers, alerting to keystrokes, keywords and inappropriate access. The monitoring and content filtering systems are monitored by the IT team who alert the safeguarding team to any alerts. These are then dealt with under normal safeguarding processes and logged via MyConcern.

The robustness of this security and filtering on our learner server will be tested Biannual on in-house learner accessible IT systems and servers is carried out using the SWGfL Test Filtering online utility at <http://testfiltering.com/> which tests against the IWF URL list, UK terrorist content (CTIRU) list and checks whether filters are blocking certain types of harmful or illegal content. Specifically, child sexual abuse material, terrorist related content, pornographic content and pages that contain profanity

There will be situations when learners will need to research topics that would normally result in internet searches being blocked, e.g. racism; drug use; discrimination; freedom of speech, etc. When such a situation is anticipated to arise, staff can request that the IT team temporarily relax the standard filter for the defined period of study only. Any request to do so must be requested in writing, with clear reasons for the need, and be authorised by The Managing Director.

Learners must be taught in all lessons to be critically aware of the website content they access on-line and be guided to validate the accuracy of information

Learners must be taught to acknowledge any source of information they cite or use and to respect copyright when using material accessed on the internet.

Email

Reflections Training Academy uses Office 365 for emails which include online projection to detect and block viruses, spam, phishing, Trojan, and other malicious message types.

All staff use standard Reflections Training Academy-issued email addresses

- a. Staff and volunteers will use only a Reflections Training Academy email account for their professional use
- b. All digital communication between staff and learners, parents/carers and employers (email, Messaging) must be professional in tone and content.
- c. Learners should be taught about email safety issues, such as the risks attached to the sharing or revealing of personal and private details and opening attachments. They should also be taught strategies to deal with inappropriate communication and be reminded of the need to write emails clearly and correctly and not include any unsuitable, illegal or abusive material.
- d. Staff and all those connected professionally with Reflections Training Academy will not send material that is illegal, obscene, upsetting, discriminatory or defamatory, or that is intended to annoy or intimidate another person. Should such content be received, it must not be forwarded to anyone and must be reported to the DSL, who will take appropriate action
- e. Users should not attempt to send any emails known to contain viruses or be considered as spam or phishing, Trojan and other malicious attachments are a danger to Reflections Training Academy systems
- f. Users should be aware that email communications may be monitored

Digital still and video images

- a. We gain written permission for use of digital photographs or video involving Learners as part of the agreement form when a learner joins Reflections Training Academy. The agreement form also requires the parent/carer signature if the learner is under 18 years of age.

- b. We do not identify learners in online photographic materials or include the full names of learners in any published company-produced video materials
- c. Staff must not take still or video images of learners with their personal mobile phones

Data security

Refer to UK-GDPR Policy

Mobile phones

- a. Staff are not permitted to use their own personal phones or devices for contacting learners and their families within or outside of Reflections Training Academy in any capacity and must only use company devices
- b. When using company mobile devices for texting or messaging purposes, messages must be of a clear and professional standard at all times. No slang or 'text chat' or abbreviations to be used.
- c. Only company authorised messaging platforms (text, WhatsApp or Esendex) to be used
- d. Only authorised Apps to be installed onto company phones

Internet and social networking sites

Staff Conduct

Staff are reminded that their professional responsibilities require them to act professionally in their social networking and internet activities and to create a clear distinction between their social and their professional lives. All new staff employed will be subject to an online digital footprint search prior to commencing their role. Contact with learners must remain within the boundaries of their professional lives and contact with learners should only be made through official Academy social media outlets. The guiding principle here is "think before you post"

(See Staff Code of Conduct)

Where staff makes use of web-publishing and social networks for professional purposes they are expected to:

- Behave professionally and with integrity
- Adhere to company guidelines
- Respect their audience
- Promote productive conversations
- Protect and enhance the value of the Academy reputation
- Protect confidential and business-sensitive information
- Be personable, add value and encourage responses
- Be proactive in correcting any errors made

Staff must not post comments or any other information on any public forum, website, social networking site or blog:

- That is unsubstantiated and/or negative about Reflections, their colleagues, our Learners, employers, or customers
- That runs counter to the Reflections Equality and Diversity, Extremism & Radicalisation and Safeguarding Policies.
- That recommend or appear to endorse lawbreaking of any kind.
- That gives an account of any inappropriate behaviour or are counter to Academy Values.
- Nor should such comments be made in emails sent in an official or professional capacity.

Communications between staff and current or prospective learners should only take place for legitimate, professional reasons. In some cases, there may be a non-professional reason for a relationship to exist beyond the academy (e.g. common vocational interest / common membership of a club, society or team/family members). In such circumstances, social communication may occur. Staff should, however, be aware of the risks involved and use their professional judgment to ensure that this communication is limited appropriately.

A member of staff inviting a current or prospective learner to join a network without any professional purpose or inviting them to 'follow' a purely personal profile will be regarded as inappropriate (see Staff Code of Conduct). The risks in this situation are clear and there can be no justification. Where such a situation arises Reflections reserves the right to act accordingly in line with company policies and handbook.

Accepting any invitation to 'friend', follow or become part of a current or prospective learner's personal network is also considered inappropriate.

We recognise staff may wish to take part in online communities also used by learners. In such cases, staff should ensure that personal information is secured and profiles kept private. Any staff member contributing under a personal profile is obliged to ensure that minimal personal information is visible under that profile.

Official Usage

As a general principle, staff should use their Academy contact details or a 'professional' profile for communication with current and prospective learners, and ensure that any communication is both professional and necessary.

Email contact with learners, employers and other stakeholders should be channelled through the Academy email system.

Reflections Training will continue to develop the use of social media for marketing, communications and training purposes.

Authorised Academy networks (group/page/blog) that exist for a clear professional purpose should be discussed with the Senior Management Team who will offer advice and guidance on what is acceptable.

Staff creating or participating in authorised networks should do so under their Reflections professional profile.

A professional profile is where a member of staff maintains an online presence explicitly for professional purposes. This profile should minimise any information which could be used to compromise the individual and should not be used to record social activity or personal opinion but may be used to record professional information or opinion. It is important that a professional profile is not added to non-professional networks or linked to the profiles of others except where the connection is professional. This might legitimately include links to learner groups but would be unlikely to include groups of friends/family.

Learners must not post comments on a social networking site or blog, or send text messages:

- That could be viewed as bullying or harassing another member of the Academy community
- That is counter to the Academy's Equality and Diversity policy or the Learner Training Agreement
- That explicitly encourages other members of the Academy community to break the law
- That is likely to bring the Reflections Training Academy into disrepute

Learners should not post photos that they might not wish others to see. Learners must not share photos that are deemed to be “youth-produced sexual imagery”. Where staff become aware of this a safeguarding concern will be raised.

Learners should not invite staff to join social networks or follow purely personal profiles.

Learners will be given guidance on the appropriate use of the internet and e-safety through induction, workshops, e-learning, and displays.

If a Learner has cause for concern regarding the use of the internet or social networking, they must report the incident immediately to a member of staff where this will be treated as a safeguarding issue.

Reflections Training Academy Website

- a. Reflections Training Academy website will be edited only by authorised staff. All information placed on the website must adhere to the ethos and values of Reflections Training Academy and only be published once authorised by a Director
- b. Personal learner information, including home address and contact details, will not be uploaded to the website
- c. The website will not publish the surnames of learners
- d. Reflections Training Academy will ensure that the image files are appropriately named – and do not use learners’ names in image files if published on the web
- e. Reflections Training Academy will ensure the web hosting company has a published security protocol.

Remote Learning Platforms

The use of technologies introduced and used due to Covid 19 pandemic and the lockdown situation the way we interact and train our learners has changed.

There are a number of online options that we are now utilising. Ranging from merely setting activities or providing access to online resources, through video tutorials, to interactive video conferencing.

The use of audio and video for real-time online training, means we need to consider the steps to safeguard staff and learners:

This policy should be read in conjunction with the “Remote & Online Learning” appendix

Online bullying

Bullying is defined in guidance issued by the Department of Education as: ‘behaviour by an individual or group, repeated over time, that intentionally hurts another individual or group either physically or emotionally’¹

What is online bullying?

Online bullying is the use of technology, for example, mobile phone, email, social networking sites, streaming platforms, chat rooms and instant messaging services, to deliberately upset someone else

- It can be used to carry out different types of bullying, as an extension of face-to-face bullying
- It can also go further as it can invade home/personal space and can involve a greater number of people
- It is an anonymous method by which bullies can torment their victims at any time of day or night
- It can draw others into being accessories

- It includes ~~threats and~~ intimidation; harassment or 'cyber-stalking'; vilification/defamation; exclusion or peer rejection; impersonation; unauthorised publication of private information or images (i.e. possible breach of copyright); and manipulation;
- It includes the consensual and non-consensual sharing of nude and semi-nude - and other explicit images electronically. These images can be subsequently widely distributed
- It also includes trolling; the practice of posting upsetting, provocative, offensive, or off-topic messages in an online community. Trolling comments are posted with the deliberate intent of provoking readers into an emotional response, or of otherwise disrupting normal on-topic discussion.

Impact on the victim

The victim may receive an email, chat, text messages or posts and direct messages on social networking sites that make them feel scared, embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their psychological wellbeing. Online bullying can pose a serious threat to their physical and emotional safety. Support for victims of online bullying will be supported by the safeguarding team, support is also available through Togetherall

Responding to online bullying

Most cases of online bullying can be dealt with through Reflections anti-bullying policies and procedures.

In all cases of online bullying make sure that you preserve the evidence and report through "MyConcern"

Some features of online bullying differ from other forms of bullying and may prompt a particular response. For example:

- Consider others involved (including viewers); they can amount to hundreds of people
- Change the victim's mobile phone number
- Report the bullying to the site where it was posted
- Try to get content removed from the web
- In some cases, the victim may be able to block the perpetrator from their sites and services
- Ask the person bullying to remove the offending content and say who they have sent it on to
- Contact the police in cases of actual/suspected illegal content.

What to do if you have concerns about a learner:

Staff and volunteers should follow the same procedures as for all other safeguarding issues and adhere to guidelines set out in Keeping Children Safe in Education 2022 statutory guidance. Reflections Training Academy require all staff to report an online bullying concern on "My Concern" as soon as possible

How we manage allegations against a member of staff:

Staff and volunteers should follow the same procedures as for all other safeguarding issues and adhere to guidelines set out in Keeping Children Safe in Education 2022 statutory guidance. Reflections Training Academy require staff to follow the Whistleblowing Procedure as detailed within the Safeguarding Policy.

Conclusion

Reflections Training Academy recognises that the use of technology, including access to the internet and ICT devices, can substantially and positively impact the quality of teaching and

learning of our learners and staff. This policy aims to ensure that all such use is done safely and appropriately

Definitions

What do we mean by 'online' - we include being connected to the internet or communicating through a wide range of devices or technologies, such as computers, laptops, mobile phones, tablet computers, hand-held devices and games consoles.

Parent/carer- refers to any individual who has legal parental responsibility for a Learner or has care of a Learner aged under 18.

DSL - Designated Safeguarding Lead

Webinar - Online delivered session via online video and audio platform such as GoToMeeting, Microsoft Teams or Zoom.

ICT -Information and Communication Technology – refers to technologies that provide access to information through telecommunications. This includes the Internet, wireless networks, smartphones, and other communication mediums and devices.

Open communication takes place in a public forum (e.g. Facebook, Instagram) which can be viewed by unknown internet users i.e. the general public

Closed communication is where the participants are all known to each other. Most closed communication will be between two individuals (e.g. email exchange) but would also include 'friends only' groups or sites with registered members etc.

Public information is that which can be accessed anonymously by internet users who are unknown to the originator.

Private information is that which is only available to a limited, known sub-set of internet users or solely by the owner of the information themselves.

The **originator** of online content is the individual who first uploads or creates the content using online tools.

Distribution - posting, uploading, adding, or forwarding digital content via electronic, web-based systems (including email and text) constitutes a distribution of that content. A choice to publicly distribute private information is the responsibility of the distributor NOT the originator or the maintainer of the system used to distribute.

It is the responsibility of content originators to understand the system they are using and, where control cannot be guaranteed, to amend the use of the system accordingly.

Useful online safety Websites

Child Exploitation & Online Protection Centre: - <http://ceop.police.uk/>

Child Exploitation & Online Protection: - <https://www.thinkuknow.co.uk/>

UK Safer Internet Centre: - <https://saferinternet.org.uk/professionals-online-safety-helpline>

Internet Watch Foundation - <https://www.iwf.org.uk/>

Internet Matters - <https://www.internetmatters.org/advice>

South West Grid For Learning - <https://swgfl.org.uk/>

https://reflectionstrainingacademy-my.sharepoint.com/personal/lucy_reflectionstraining_co_uk/Documents/Lucy/Policies and Procedures 2024/Safeguarding/SG Policy Appendix 5 - Online Safety policy - Version 18.docx

