ONLINE SAFETY POLICY

Version number	Purpose/Change	Lead	Review date	Next review
3	Annual Review	Sarah McCarthy	20.10.2023	Nov 2024
2	Annual Review	Gina Stephens	11.08.2022	Sept 2023
1	New Policy	Sam Wilson	10.01.2022	Mar 2023

INTRODUCTION

The use of technology has become an established and integral part of learning through the use of online resources, online delivery, and remote working. Learners and staff have access to technology and resources that have a significant and positive impact on learning. Young people need to develop good skills in using technology to maximise its use as a learning tool and prepare themselves for future employment and careers. Technology is established as a supportive tool in good teaching and learning however, it has also established itself as significant component of many safeguarding issues.

PURPOSE

- Ensure the safety and wellbeing is paramount when staff and learners are using the internet, social media or mobile devices.
- Provide staff, learners and volunteers, with the overarching principles that guide our approach to online safety.
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

We believe that:

- Our learners and staff should never experience abuse of any kind.
- Our learners and staff should be able to use the internet for education and personal development, but safeguarding procedures need to be in place to ensure they are kept safe at all times.

We recognise that:

- The online world provides everyone with many opportunities; however, it can also present risks and challenges.
- We have a duty to ensure that all young people and adults involved in our organisation are protected from potential harm online.
- We have a responsibility to help keep learners safe online, whether or not they are using the company's network and devices.
- Working in partnership with learners, their parents, carers and other agencies is essential in promoting their welfare and in helping learners be responsible in their approach to online safety .
- Regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, we all have the right to equal protection from all types of harm or abuse.

POLICY SCOPE

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments within the Company, emerging themes or trends within the wider community or any changes in national guidance.

This policy applies to all staff, learners and other stakeholders who have access to our digital technology, networks and systems, whether on-site or remotely, or who use technology in their role and should be read alongside the IT Policy, Online Code of Conduct and Acceptable Use of Technology Policy.

Learners are responsible for using any IT systems and mobile devices of the Company, in accordance with the online safety rules. Learners must act safely and responsibly at all times when using the internet and/or any mobile technologies. Online safety is embedded within the curriculum, including online safety modules for all learners to complete as part of their induction so they have an understanding of online safety and know how to act in line with the Company's policies regarding mobile phone use, sharing images, cyber-bullying etc. They must follow reporting procedures where they are worried or concerned, or where they believe an online safety incident has taken place involving them or someone else they know.

Staff are responsible for using IT systems and mobile devices in accordance with the online safety rules, which they must sign and submit to the Company's Head of Digital and ICT. Staff are responsible for attending staff training on online safety and displaying a model example to learners at all times through embedded good practice.

All digital communications with learners must be professional at all times and be carried out in line with this policy. Online communication with learners is restricted to the Company's professional networks via Microsoft platforms such as Teams and Outlook and e-portfolio systems. External platforms not hosted by the Company's, may never/be used unless express permission from the IT department is obtained.

POLICY AIMS

- To set out expectations for online behaviour, attitudes and activities and use of digital technology (including when devices are offline) for all staff and learners.
- Help all to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the organisation regardless of device or platform.
- Facilitate the safe, responsible, and respectful use of technology to support teaching and learning, increase attainment and prepare all learners for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help staff working with learners to understand their roles and responsibilities, to work safely and responsibly with technology and the online world for the protection and benefit of themselves and that of the learners, minimising misplaced or malicious allegations and to better understand their own standards and practice.
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns with reference to other policies such as Behaviour Policy or Anti-Bullying Policy.

SECURITY

The Company will do all that it can to make sure the network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, workstations etc. to prevent accidental or malicious access of the Company's systems and information. Digital communications, including email and internet posting will be monitored by IT department.

RISK ASSESSMENT

In making use of new technologies and external online platforms, IT department must first carry out a risk assessment for online safety. A risk assessment must also be carried out where a learner is learning off site e.g., on work placement.

BEHAVIOUR

The Company will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and investigated in line with the learner and staff disciplinary procedures. Where conduct is found to be unacceptable, the Company will deal with the matter internally. Where conduct is considered illegal, the Company will report the matter to the police or local safeguarding authorities, as appropriate.

COMMUNICATIONS

There are a variety of technologies and sites now available through which individuals can communicate with one another. The Company's IT department agrees with users' permissions and when and how these technologies may be used and update decisions in line with the evolving nature of ICT.

The Company requires all users of IT to adhere to the relevant policies which states clearly when email, mobile phones and social media sites may be used.

This policy can only impact upon practice if it is a (regularly updated) living document. Therefore, it is accessible to and understood by all stakeholders. It is communicated in the following ways:

- Posted on the organisation's website.
- Included in induction of staff and learners.
- Integral to safeguarding updates and training for all staff.
- Clearly reflected in the Online Code of Conduct and Acceptable Use Policies for staff and learners which are issued during induction and updated/reviewed annually.

USE OF IMAGES AND VIDEO

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or learners.

No image/photograph can be copied, downloaded, shared or distributed online without permission. Learners are not permitted to take photographs or videos in lessons, unless part of a learning activity and authorised by the given tutor. Approved photographs should not include names of individuals without consent.

PERSONAL INFORMATION

Personal information is information about a particular individual. The Company collects and stores the personal information of learners and staff regularly e.g., names, dates of birth, email addresses, assessed materials and so on. The Company will keep that information safe and secure and will not pass it onto anyone else without the express permission of the learner/parent and/or guardian.

No personal information can be posted to the Company's website without consent unless it is in line with our GDPR/Data Protection Policy. Only names and work email addresses of (senior) staff may be used on The Company's website - no staff or learners' personal information will be available on the website without consent.

Staff must keep learners' personal information safe and secure at all times. When using an online platform, all personal information must be password protected. Every user of IT facilities is required to log off on completion of any activity or lock their device where they are physically absent from a device for any period of time.

KEEPING STAFF AND LEARNERS SAFE

We will seek to keep staff and learners safe by:

- Appointing an Online Safety Coordinator.
- Providing clear and specific directions to staff and volunteers on how to behave online through our Online Code of Conduct and Acceptable Policy Use for staff and learners.
- Online safety and expectations when using technology for teaching and learning is discussed at induction.
- Through our teaching and learning, provide learners with the support, encouragement and information to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- Where appropriate supporting and encouraging parents and guardians to do what they can to keep their children safe online.
- The use of 'acceptable use agreements' understood and signed by staff.
- Developing clear and robust safeguarding procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by a staff member or learner.
- Reviewing and updating the security of our information systems regularly.
- Ensuring that usernames, logins, email accounts and passwords are used effectively.
- Ensuring personal information about the learners who are involved in our organisation is held securely and shared only as appropriate.
- Providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation.

INCIDENTS AND RESPONSE

Where an online safety incident is reported, this matter will be dealt with very seriously. The Company will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring.

Where any report of an online safety incident is made, the safeguarding procedure is followed:

- All members of staff are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through our safeguarding procedures and where necessary liaise with employers.
- For reporting concerns, the 'logging a concern form' is used for logging the details of those events. The form will be submitted to the designated safeguarding lead.
- If appropriate parents/guardians of online-safety incidents involving their child will be notified and Children Social Care/ Police where staff or learners engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and up skirting; see section below).
- Any concern/allegation about staff misuse is referred to the DSL unless the concern is about these individuals in which case the concern will be referred to the Managing

Director. Safeguarding procedures for dealing with an allegation against a staff member will be followed, advice and support will be sought form the LADO (Local Authority's Designated Officer) if appropriate.

- Reviewing at regular intervals any support plan developed to address online abuse, in order to ensure that any problems have been resolved in the long term
- Concerns will be handled in the same way as any other safeguarding concern following established and robust safeguarding procedures for responding to abuse (including online abuse).
- Making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account.

What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct (identified by Professor Tanya Byron's 2008 report "Safer children in a digital world"). These three areas remain a helpful way to understand the risks and potential response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

Many of these new risks are mentioned in KCSIE 2023, e.g. extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families including sexual exploitation, criminal exploitation, serious youth violence, up skirting and sticky design.
In past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation (CSE, CCE and radicalisation) as more time is spent at home and on devices. There is a real risk that some learners may have missed opportunities to disclose such abuse during the lockdowns or periods of absence.

Sexting – sharing nudes and semi-nudes
Refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people for education settings to avoid unnecessary criminalisation of children.

NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called Sharing nudes and semi-nudes: https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-how-to-respond-to-an-incident-overview on how to respond to an incident for all staff to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken.

Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The DSL will in turn use the full guidance document, 'Sharing nudes and semi-nudes advice for educational settings' to decide next steps and whether other agencies need to be.

Up skirting:

- It is important that everyone understands that up skirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence.

Bullying :

- Online bullying should be treated like any other form of bullying and the bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

Sexual violence and harassment:

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education (2023) and also a document in its own right. All staff must read Part one of this document as a minimum: paragraphs 51-57 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise. Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance.
Staff must work to foster a zero-tolerance culture. The guidance stresses that education settings must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language

MONITORING AND REVIEW

The impact of the policy will be monitored regularly with a full review being carried out at least on an annual basis. The policy will also be reconsidered where particular concerns are raised or where an online safety incident has been recorded.