POL-QUA-49

Online Safety Policy

Policy Reference	Version	Policy Owner	Next Review Date
POL-QUA-00	**V5**	**Karenza Morgan**	**June 2025**

Current Author	**Karenza Morgan**
Author's Job Title	**Designated Safeguarding Lead**
Department	**People and Culture**
Document Status	**Draft / Approved**
Date Approved	**24/6/2024**
Approved By	
Classification Level	
Priority Level Review required Red - within 1 year; Amber – within 2 years; Green - within 3 years	**Red**

Distribution

All Futures employees, volunteers and apprentices, subcontractors, grant recipients and customers.

Related Policies	

Version	Date	Author	Author's job Title	Changes
V5	24/06/2024	KM	DSL	Move onto new template and annual review

For Information: Where we refer to as 'Futures' in this policy – we are referencing a group of companies made up of Futures Advice, Skills & employment Ltd and Nottingham & Nottinghamshire Youth Support Ltd

To keep things simple throughout this document, ‘we’ and ‘us’ means the Group Companies and its associated brands. This policy applies across all companies within the Group.

1 Online Safety Context/Policy Statement

1.1. Futures recognises the benefits and opportunities which new technologies offer to staff, customers, learners and stakeholders. We provide internet access to all customers, learners and staff accessing services within our premises and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet, social media and different technologies available mean that we are also aware of potential risks and challenges associated with such use.

2.1. It is essential that children and adults at risk are safeguarded from potentially harmful and inappropriate material or behaviours online. Futures will adopt a whole organisational approach to online safety which will empower, protect, and educate our customers, learners and staff in their use of technology, and establish mechanisms to identify, intervene in, and escalate any concerns where appropriate.

3.1. Futures identifies that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

1.1.
2.1.
3.1.

1.3.1. Content: being exposed to illegal, inappropriate or harmful content. For example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

2.3.1. Contact: being subjected to harmful online interaction with other users. For example, child on child abuse, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

3.3.1. Conduct: personal online behaviour that increases the likelihood of, or causes, harm. For example, 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 and online bullying.

4.3.1. Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

2 Overall Aim and Objectives

2.

1.1. Futures recognises that technology, and the risks and harms related to it, evolve and change rapidly. Futures will carry out an annual review of our approaches to online safety, supported by an annual risk assessment which considers and reflects the risks our customers, learners and staff face.

2.1. This policy applies to all members of Futures (including staff, customers, learners, volunteers, and Stakeholders) who have access to and are users of Futures ICT systems, both in and out of the organisation.

3.1. We have a responsibility to help keep children, young people and adults safe online, whether or not they are using Futures network and devices

4.1. This is pertinent to incidents of cyber-bullying, exposure to inappropriate content or other online safety incidents covered by this policy, which may take place outside of the premises but are linked to users of Futures ICT systems or services. Futures will provide access to resources and training to raise awareness for uses in areas set out in section 3. Definitions.

5.1. Our approach is to implement appropriate safeguards within the company, while supporting those who use technology to identify and manage risks independently and with confidence.

6.1. Whilst regulation and technical solutions are very important, there use must be balanced by educating users to take a responsible approach. Education in online safety is therefore an essential part of Futures online safety provision. Futures helps and supports children, young people and adults to recognise and avoid online safety risks and build their resilience. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies.

7.1. Futures will do all we reasonably can to limit customers/learners and staff exposure to online risks through provided IT systems and will ensure that appropriate filtering and monitoring systems are in place.

8.1. In furtherance of our duty to safeguard, we will do all that we can to make our customers, learners and staff stay safe online and to satisfy our wider duty of care. Online safety will be a focus in all areas of the business and staff should take active steps to reinforce online safety messages across services.

9.1. We will do this through raising awareness of potential risk and embedding online safety awareness into our everyday practice through:

1.3.1. How to use technologies in a safe and responsible way
2.3.1. Supporting and encouraging the young people and adults using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
3.3.1. Provide online safety agreements for use with staff and volunteers, young people and their parents/carers and adults using our online services
4.3.1. Provide clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person.
5.3.1. Providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code.
6.3.1. Reviewing and updating the security of our information systems regularly
7.3.1. Ensuring that usernames, logins, email accounts and passwords are used effectively
8.3.1. Ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
9.3.1. Ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
10.3.1. Providing supervision, support and training for staff and volunteers about online safety
11.3.1. Examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

3 Definitions

2.

3.

1.1. Cyberbullying

1.1.1. Cyberbullying or online bullying can be defined as the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else. It is often linked to discrimination and like other forms of bullying, affects self-esteem and can affect mental health and wellbeing. Addressing all forms of bullying and discrimination is vital to support the health and wellbeing of the Futures community.

2.1. Unsafe Communities

1.1.1. An online community can act as an information system where members can post, comment on discussions, give advice or collaborate. Commonly, people communicate through social networking sites, chat rooms, forums, e-mail lists and discussion boards. People may also join online communities through video games, blogs and virtual worlds.

2.1.1. Users also need to be aware of the dangers of unsafe communities such as extremist and criminal groups

3.1. Use of Digital and Video Images

1.1.1. Futures recognises the specific risks that can be posed by mobile and smart technology, including mobiles/smart phones, cameras, wearable technology. In accordance with KCSIE2023 Futures has appropriate mobile, smart technology and image use information contained within this and the safeguarding policy, which is shared and understood by all staff.

2.1.1. The development of digital imaging technologies has created significant benefits to work and learning, allowing the use of images that have been recorded or downloaded from the internet. However, customers, learners, staff and stakeholders need to be aware of the risks associated with publishing inappropriate content on the internet. Such images may provide avenues for cyber bullying, child on child abuse, child sexual exploitation, sexual violence & sexual harassment or grooming to take place.

3.1.1. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. Futures will inform and educate users about these risks to reduce the likelihood of the potential for harm.

4.1. Sexting/Sharing nudes and semi nudes

1.1.1. Sexting is when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages. They can be sent using mobiles, tablets, smartphones, and laptops - any device that allows you to share media and messages. This includes videos or live streams via social media, gaming platforms, chat apps or forums. It could also include sharing between devices via services like Apple's AirDrop which works offline.

2.1.1. Guidance for sharing nudes and semi nudes in KCSIE 2023 is not about:

- Images of under-18s created by adults (refer to police for this)
- Under 18s sharing adult pornography
- Exchanging text-only sexual content

3.1.1. The KCSIE 2023 and UKCIS 2020 guidance is about

- Risk assessing situations
- Safeguarding and supporting children and young people
- Handling devices and images
- Recording incidents, including the role of other agencies
- Informing parents and carers

4.1.1. If handled poorly an unsafe and unhealthy set of norms can be created which enable child on child abuse and this can also prevent other children and young people from disclosing.

5.1.1. Making, possessing and distributing any imagery of someone under 18 which is indecent is illegal. The Sexual Offences Act 2003 defines a child for the purpose of indecent images as anyone under the age of 18. The non-consensual sharing of private sexual images or videos with the intent to cause distress is also illegal. However young people should not be unnecessarily criminalised.

6.1.1. Futures recognises that consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as youth produced/involved sexual imagery or "sexting") can be a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

7.1.1. In many cases, educations settings may respond to incidents without involving the police, for example where an incident can be defined as experimental. However, where there are abusive or aggravating factors, incident should always be referred to the police through the local safeguarding partnerships.

- Aggravated Incidents – Incidents involving additional or abusive elements beyond the creation, sending or possession of nudes and semi-nudes

- Experimental Incidents – Incidents involving the creation and sending of nudes or semi-nudes with no adult involvement, no apparent intent to harm or reckless misuse.

8.1.1. Further information on safeguarding concerns in this are included in the safeguarding policy

5.1. Online predators/Grooming

1.1.1. When users go online, they have direct and immediate access to friends, family, and complete strangers, which can put unsuspecting children, young people and adults at great risk. Children and young people who meet and communicate with strangers online are easy prey for Internet predators. Predators have easy and anonymous access to children online where they can conceal their identity and roam without limit. Today's sexual predators search for victims while hiding behind a computer screen, taking advantage of the anonymity the Internet offers

2.1.1. Children's posts or profile information may expose personal information and put them at risk. For example, they may talk about their home life, feelings, or thoughts they've been having. There may be information that makes them identifiable such as locations of events they are taking part in or visual clues in photographs. Perpetrators may use this information to groom, abuse or exploit children.

3.1.1. Perpetrators of abuse may create fake profiles to try to contact children and young people through the platform you're using, for example an adult posing as a child. They may also create anonymous accounts and engage in cyberbullying, grooming or trolling. People known to a child can also perpetrate abuse

6.1. Cybercrime

Common forms of cybercrime include:

- phishing: using fake email messages to get personal information from internet users;
- misusing personal information (identity theft);
- email scams set up to commit theft through banking
- hacking: shutting down or misusing websites or computer networks;
- spreading hate and inciting terrorism;
- distributing child pornography;
- grooming: making sexual advances to minors.

4 Prevent Duty and Radicalisation

4.

1.1. As we become a more digital society radical or extremist views become more accessible via the internet. Access to vulnerable individuals has become easier due to the increased use of social media. As a result, the identifiers of someone becoming radicalised are similar to those of someone experiencing grooming.

2.1. Millions of young people use social media platforms every day to share content, but there are a growing number of users who exploit it to radicalise and recruit vulnerable people. The Internet has played a significant role in the radicalisation and recruitment of foreign fighters and continues to do so. Social networking is the main activity young people aged 16-24 use the internet for, something which extremist groups are well aware of using platforms such as Facebook, X (Twitter), WhatsApp, Snapchat, Discord, Gab, VK, Parler, Telegram and YouTube (to name a few) to draw young people to their cause.

3.1. Extreme Far Right and Islamist extremist groups are using the Internet to recruit 'a new younger generation of members'. It is also facilitating the ability of extremist groups to organise and promote themselves.

4.1. There is a wealth of Extreme Far Right and Islamic extremist material available online including; articles, images, videos encouraging hate or violence, posts on social media and, websites created or hosted by terrorist organisations. There are also terrorist training materials and videos glorifying war and violence that play on the theme of popular video games such as 'Call of Duty: Black Ops'. These use highly emotive language and images created to play on the issues young people are struggling with such as identity, faith and belonging.

5 Acceptable Use Policies (AUP)

5.

1.1. Futures acceptable use policies are intended to ensure that all users will be responsible and stay safe while using Futures internet and other digital technologies. Futures systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

2.1. Futures Acceptable Use Policy/Agreements are attached as an annex to the IT and Data Security Policy and will be signed by all users of Futures ICT systems.

3.1. All ICT staff are responsible for ensuring that they have an up-to-date awareness of online safety matters and of Futures online safety policy and practices and have read, understood and signed the Acceptable Use Policy (AUP).

4.1. Customers/Learners that use Futures IT systems or equipment must also sign Futures Acceptable use agreement (customer/learner/guest version).

5.1. Social Media – Protecting Professional Identity

1.1.1. User agreements set out the expectations about the appropriate use of social media. This guidance must be followed in order to ensure that users do not engage in any activity which may cause them to breach acceptable standards of conduct

6 Roles, Responsibilities and Structure:

The following section outlines the broad online safety roles and responsibilities of individuals and groups within Futures.

6.

1.1. Futures Board

1.1.1. Futures Board is responsible for the overall effectiveness of the policy. This will be carried out by the Board receiving regular information about online safety incidents and monitoring reports. A member of the Board has the role of Safeguarding Champion, which includes online safety.

2.1. Designated Strategic Safeguarding Lead (Operations Director) (DSSL)

1.1.1. The DSSL has a duty of care for ensuring safety within Futures and therefore has overall responsibility for online safety within the organisation but will liaise with other members of staff, for example DSL for policy and procedures, IT technicians, operational leads etc. as necessary.

3.1. Designated Safeguarding Lead (DSL)

1.1.1. The DSL will respond to online safety concerns reported in line with our safeguarding and other associated policies, including our harassment and bullying, social media and behaviour policies.

4.1. Senior Leadership Team/Online Safety Group

1.1.1. The DSSL delegates much of the day to day responsibility for online safety to the DSL and senior function heads who form the Online Safety Group. The Online Safety group has a leading role in establishing, reviewing and implementing Futures online safety procedures, providing training and advice for staff. Designated safeguarding officers liaise with outside bodies in relation to online safety issues.

5.1. Users of Futures ICT systems

1.1.1. Users of Futures ICT systems include learners, apprentices, customers, subcontractors, employers and other external stakeholders.

2.1.1. Users of Futures ICT systems should be aware of the significant risks of exposing themselves or others to personal harm or danger because of inappropriate use of IT and digital media and should manage their use of IT to minimise these risks.

3.1.1. Users are responsible for using Futures IT systems in accordance with their IT user agreements and generally understanding the importance of adopting good online safety practice when using digital technologies in and out of the organisation.

6.1. Staff

1.1.1. Staff that work directly with customers and learners are also responsible for helping them understand the importance of online safety and how they can reduce exposing themselves to risk and unsuitable content which includes, but is not limited to, adult material, gambling, drugs, discrimination, racism, violence, child on child abuse, sexual violence and sexual harassment, terrorism and extremism.

2.1.1. Any reported incident of unacceptable conduct will be treated seriously and in line with other relevant policies and procedures.

7.1. ICT Technical Support Staff

1.1.1. The ICT team is responsible for ensuring that Futures' technical infrastructure is secure and is not open to misuse or malicious attack. Appropriate filters, monitoring and password protection is in place to reduce the risk of online safety issues arising.

2.1.1. The ICT team will monitor usage of the internet through the installation of software on all company devices and through the network, allowing the team to monitor usage and users on the internet and restrict access to illegal, harmful or inappropriate images and content. Inappropriate use of internet will be reported through monitoring reports to the Safeguarding Lead and Operations Manager.

3.1.1. The ICT team are responsible for undertaking risk assessments on any new technology or software introduced in order to consider the online safety risks to users.

7 Online Safety Procedures:

7.

1.1. User Agreements, (included in the IT and Data Security Policy) set out the requirements in relation to appropriate use of technology and the internet and reporting unsuitable or inappropriate activities. Where such activities also raise a safeguarding concern, Futures' Safeguarding Policy, and relevant procedures must be followed.

2.1. It is more likely that Futures will need to deal with incidents that involve inappropriate rather than illegal misuse. Incidents will be dealt with as soon as possible in a proportionate manner and users will be made aware that incidents have been dealt with. Incidents of misuse will be dealt with through company behavior and disciplinary procedures.

8 Online Safety training and continuous professional development

8.

1.1. All staff will receive training on company policies and procedures relating to safeguarding and online safety and will be made aware of the local safeguarding arrangements as part of the company induction. Ongoing online safety training and updates for all staff, customer and learners will be integrated, aligned and considered as part of our overarching safeguarding and Prevent Duty approach.

2.1. All staff will be required to undertake online Safety training depending on their role as part of their induction. This includes all managers who are involved in managing teams who are customer facing.

3.1. All staff will have access to resources to support awareness of online safety through intranet, extranet and local resources.

4.1. Futures will ensure a response is in place to enable all learners to learn about and manage online risks effectively as part of providing a balanced curriculum.

9 Policy Monitoring and Evaluation

9.

1.1. The Online Safety Group comprising of Futures DSL (lead), Designated Persons and Functional Managers will conduct an annual review of our online safety systems and policies. This will include consideration of specific cases dealt with by staff in the last year. The resulting information, including feedback from staff, will be used by the designated person to inform any improvements necessary. Quarterly online safety reports will be reviewed at Futures Board level.

2.1. Futures online safety policy and procedures will be clearly communicated to staff, learners, volunteers, subcontractors, Board Members and Service Users through the use of the company, intranet and extranet and our communications department. The Designated Safeguarding Officer: Policy and Procedures named person will be responsible for ensuring this is done.

10 List of related strategies, policies, and procedures

10.

1.1. The policy should be read in conjunction with the following strategies, policies and plans in the policy section of the intranet:

1.1.1. IT and Data Security policy, including employee/learner user agreement
2.1.1. Data Protection Policy
3.1.1. Health and Safety
4.1.1. Safeguarding Policy and Procedures
5.1.1. Harassment and Bullying Policy
6.1.1. Managing Allegations of abuse against staff Policy
7.1.1. Whistleblowing Policy
8.1.1. Mobile Phone Policy
9.1.1. Photography and image sharing guidance
10.1.1. Code of Conduct for staff and volunteers

Annex 1 Guidance on Responding to Online Safety Incidents

Annex 2 - Guidance for Remote Interactions with Young People and Adults at Risk

1. Background

1.1. During any period of uncertainty, it's essential that we continue to maintain contact with our customers to support them during important transition periods such as progression to Post 16 or Post 18 learning, training or employment. However, this work will take different forms that require additional thought to ensure that both customers and practitioners are appropriately safeguarded.

2.1. Any of the current safeguarding procedures need to be adhered to, any practitioners conducting one -to one interactions have undertaken safeguarding training and adhere to statutory safeguarding guidance. All practitioners should make themselves aware of who the Designated Safeguarding Officer (DSO) is, how to contact them and how to make safeguarding referrals during this time.

3.1. Practitioners and management should discuss and agree:

1.3.1. All aspects of planning for and scheduling of one-to-one virtual sessions.

2.3.1. Methods of delivery that enable all customers to take part regardless of access to technology, disability and environment.
3.3.1. An appropriate process in the event of a crisis arising during an online one-to-one session.
4.3.1. Procedures to notify customers of their appointment in advance including how to access the technology.
5.3.1. Methods of informing parent/carers/guardians of the remote support available, where required – this could also include signposting links to other trustworthy organisations.
6.3.1. Consent is still necessary to complete with all customers as you would normally in face-face interactions and should be recorded in the normal ways. Managers and teams need to discuss ways of capturing this such as receiving email or text consent response to a standard consent statement sent and then the whole conversation being recorded.

2. Remote delivery can include:

1.
2.

1.1. Real time methods e.g.

1.1.1. Video (Skype, Zoom, WhatsApp, Microsoft Teams. Google Hangouts etc)
2.1.1. Telephone, Instant chat

2.1. Delayed response

1.1.1. E-mail, letter. Text

3. Agreement

3.

1.1. Practitioners should ensure that the agreement part of the interaction takes place – even where the adviser has previously engaged with the customer – and that it is clear and understood. This should include basics on the core areas such as Safeguarding (confidentiality, disclosure), GDPR (recording) – as well as time of the interview and the ethics of a good interaction e.g. explore all options, the ability for the customer to leave if they wish, be honest, ask questions

4. Good practice for virtual meetings

1.1. **Disclosure: students sometimes disclose information and emotion very quickly online. Practitioners need to understand the dynamics underpinning this kind of response so that they can work effectively with students who exhibit this**.

2.1. Risk Assessment: practitioners should assess each situation before the session and also pro-actively during the session to assess the risk to themselves and the young person and take action or change their approach accordingly.

3.1. Most meetings should be held within an agreed timeframe (e.g. normal school times or working hours though not exclusively) and not exceed the normal duration of a face to face interaction (e.g. 45 minutes) except in exceptional circumstances

4.1. A record of each meeting should be kept. This should include the method of delivery and summary of the discussion and any actions that were agreed. All records must be kept secure in line with usual GDPR requirements.

5.1. Where possible where having contact in 1:1 situations with a child, young person or an adult at risk – ensure a parent, teacher or other facilitator can be invited to the meeting and drop in from time to time.

6.1. Make sure the platform you are using is suitable for their age group. Also check the privacy settings so that it is secure as possible from outside hacking.

7.1. All practitioners and customers must wear suitable clothing, including anyone else in the household.

8.1. Any devices used should be in appropriate areas, for example, not in bedrooms. Consider the background that the customer will see on video.

9.1. Language must be professional and appropriate, including that of any family members in the room.

10.1. Webinars and live broadcast should be recorded where possible to maintain a record of the activity. You will need to store this in line with GDPR requirements. This is possible in teams and some apps, further guidance will follow.

5. CPD

1.1. Practitioners should be honest about their skills and knowledge regarding conducting remote interactions. This should include their ability to use technology effectively and an awareness of how electronic data and information are stored, along with the ethical and legal requirements of service delivery. They should ask line managers for advice and support if they are not confident in these areas.

6. References and other sources of information

1.1. The Department for Education released the following safeguarding guidance for schools and colleges during the Covid-19 situation.
https://www.gov.uk/government/publications/covid-19-safeguarding-in-schools-colleges-and-other-providers/coronavirus-covid-19-safeguarding-in-schools-colleges-and-other-providers

2.1. The UK Council for Internet Safety (UKCIS) has published a framework and tool for organisations, to use to embed digital resilience thinking into their products, education and services. Digital resilience helps individuals recognise and manage the risks they come across when they socialise, explore or work online.
What is digital resilience?