 **Promise Care Services Ltd**

# SERVICE USER ONLINE SAFETY

**Scope**

* **Policy Statement**
* **The Policy**
* **Related Policies**
* **Related Guidance**
* **Training Statement**

**Policy Statement**

# The purpose of this policy is to:

# Ensure when service users are using the internet, social media, or mobile devices they are supported to keep safe and their wellbeing is protected.

# Provide staff and volunteers with the overarching principles that guide our approach to online safety.

# Ensure that we operate following our organisation’s ethical values and within the law in respect of how we use online devices and services.

# Apply the policy to all staff and service users or anyone involved in internet activities and support when delivering services.

Recognise that the world wide web provides people with many opportunities but it can also present risks and challenges.

Recognise that we have a duty to ensure that all adults involved in our organisation are protected from potential harm online.

Understand we have a responsibility to keep our service users safe online, whether or not they are using the organisation’s network and devices.

Support our service users to be responsible in their approach to online safety.

**The Policy**

When supporting each service user to access online content and supporting their safety, we will do so in line with their personal choices, needs and the Mental Capacity Act 2005.

In support of each service user, we will provide a range of activities and information relevant to their needs, which prepare and support the individual’s safety online including:

**Risk Assessment**

Our risk assessment aims to anticipate the main area of risks that an individual might encounter when accessing the web. Given the nature of their disability and the type of use, we will put in place the support required to mitigate any identified risk for individual service users.

**Staying Safe Online**

Staff will inform and support service users to consider the following:

* **Use secure passwords**. Websites such as Get Safe Online have information about how to choose a secure password.
* **Check privacy settings**. Just because a site requires a login, this does not necessarily mean that their profile is entirely private – some parts might still be shown publicly.
* **Think about who will see what they share**. For many people, sharing their feelings online can be helpful during a difficult time. However, some people find that when they are feeling better, they regret how much they shared, or who they shared this with. Very few sites are 100% private, and information is often shared online beyond anyone’s control. It is very difficult to remove something from the internet permanently.
* **Protect personal details**. What is shared online can affect both their privacy and the privacy of others, so it is important to think carefully about what is posted. Personal details found on social media has been used in Phishing and other scam activities to defraud people of their money. Avoid posting personal details online, like an address or telephone number. Photos or online check-ins can also give away personal information, not just written posts.
* **Fraud.** If staff or the service user thinks that someone has used their information to commit fraud, such as opening a bank account or obtaining documents, you should report it as soon as you can to the manager.
* **Protect themselves from excessive online spending**. It is very easy to spend money online. Impulsive decisions about money can also be an issue during periods of depression or unhappiness. This can lead to spending that can cause debt.
* **Dealing with triggering content**. If they come across something that upsets them, close the screen, or scroll quickly past it. They might even want to turn off their computer or mobile device and take a break. Some people find that using a distraction technique also helps, such as focusing on their breathing, watching television, or doing something else. If the service user finds themself in a bad place or having negative thoughts after seeing triggering content, they need to know they can get support from staff.
* **Be extra careful with sexually explicit content**. It is possible that someone could use it to try to harm the service user in the future. Although this does not happen often, it is something to keep in mind before sexually explicit content is shared with anyone – even privately. Victims of blackmail because of sexually explicit content, will be supported to report this to the police immediately.

**Cyber bullying**

Service users are informed and supported not to tolerate cyberbullying. They should:

* Inform a staff member immediately.
* Never respond.
* Block or delete the person.
* Keep records of any posts or messages.
* Report to the site moderators.
* Talk it over with a friend or family member.
* Be treated as a safeguarding matter.

**Meeting Someone offline**

The internet can be a great place to make connections with new people and the service user may want to take it offline. This might mean talking over the phone or arranging to meet face-to-face. Many people have established long-lasting and supportive friendships this way, but it is also important that the service user knows how to keep themselves safe.

Service users need to be aware of the dangers of meeting people offline and be supported to discuss it with staff or family and to never meet an online friend without first discussing it with a staff member.

Online learning, support and leisure activities can be extremely helpful and enjoyable, but we encourage our service users to find a balance between their online and offline life to stimulate their mental health and wellbeing.

**Staff Awareness**

This organisation will ensure its staff are aware of the potential dangers that the internet poses to our service users by:

* Knowing the latest online threats, risks and trends in online communications and social networking.
* Consider the use of technology by our service users to maintain contact with loved ones which may impact their wellbeing.
* Implement clear boundaries and structure interventions that support the appropriate use of technology.
* Offer guidance and support in navigating the online world safely.
* Provide an appropriate level of filtering and monitoring which safeguards young people from risky online content and contact.
* Ensure that those with communication difficulties have information provided in
* the format of choice and to check their understanding.

**What to do if you suspect a service user is an online abuser?**

As well as being victims of cyber abuse or crime, vulnerable service users can sometimes be the perpetrators of such acts. If you suspect this you must report this to the manager following the organisation standards adult safeguarding procedures.

**Staff befriending Service Users on Social Media**

In line with the company’s Professional Boundaries policy under normal circumstances, it is not appropriate for staff to befriend or be friends with service users and their family on any social media platform, unless this is required within their care assessment and care plan, and the Registered Manager has agreed to this in writing and it is included within the care plan.

Each exception will be risk assessed and monitored to ensure professional boundaries are being maintained, and that at no point is the service user or the member of staff at risk.

**Related Policies**

Adult Safeguarding

Cyber Security

Person Centred Planning

Mental Capacity Act

Professional Boundaries

**Related Guidance**

Safeguarding Hub [https://safeguardinghub.co.uk/category/online-safety/](about:blank)

Action Fraud. [https://www.actionfraud.police.uk/](about:blank)

Mind [https://www.mind.org.uk/media-a/2932/online-mental-health-2018.pdf](about:blank)

**Training Statement**

All staff, during induction, are made aware of the organisation's policies and procedures, all of which are used for training updates. All policies and procedures are reviewed and amended where necessary and staff are made aware of any changes. Observations are undertaken to check skills and competencies. Various methods of training are used including one to one, online, workbook, group meetings, individual supervisions and external courses are sourced as required.

Date Reviewed: May 2023

Person responsible for updating this policy: **IFEYINWA ODOEMENAM**

Next Review Date: May 2024