**E-Safety Policy**

The welfare of the child and/or vulnerable adult is paramount. Within the context of this policy ‘child’ and ‘children’ can also be taken to cover vulnerable adult(s).

GHQ Training Ltd is committed to promoting the welfare of all learners. It is the duty of all staff members to play an active role in ensuring this. All staff members are expected to be aware of their duty to report concerns.

* ***N.B. A child is defined as a person under the age of 18 years (The Children Act 1989).***
* ***A vulnerable adult is defined as a person who: “may be in need of services by reason of mental or other disability, age or illness: and who may not be able to take care of him or herself, or is unable to protect him or herself against significant harm or exploitation.” (Who Decides, Lord Chancellor’s Department 1997)***

**Introduction**

This policy provides guidance on effective approaches to e-safety at GHQ Training. It covers:

* **Policies and guidance** to enable all staff to support the e-safety of children, young people and vulnerable adults.
* **The responses** necessary when a risk to a child, young person or vulnerable adult is discovered.
* **Awareness raising** for children, young people, vulnerable adults and GHQ staff and volunteers so that they are able to keep themselves, as well as those in their care as safe as possible when using the internet and other electronic communication technologies.

**Background**

**Definition:** e-safety is defined as being safe from risks to personal safety and well-being when using all fixed and mobile devices that allow access to the internet as well as those that are used to communicate electronically. This includes personal computers, laptops, mobile phones and gaming consoles such as Xbox and PlayStation.

Safeguarding against these risks is not just an ICT responsibility, it is everyone’s responsibility and needs to be considered as part of the overall arrangements in place for safeguarding and promoting the welfare of children, young people and vulnerable adults.

**Duty of Care**

As part of the ‘Every Child Matters’ agenda set out by the Government (Education Act 2002 and the Children Act 2004) and the ‘No Secrets’ agenda, produced by the Government in 2000, it is the duty of all organisations to ensure that children, young people and vulnerable adults are protected from potential harm.

In order to do this, vulnerable individuals within our setting need to be involved in the safe use of on-line technologies. It is also important that the staff who work with these individuals are clear about safe practices so that they are safeguarded from misunderstanding or being involved in possible allegations of inappropriate behaviour.

Children, young people and vulnerable adults need to use their common sense when it comes to things they read, hear and see. In the same way that the quality of information received via radio, newspaper and television is variable, everyone needs to be helped to develop skills in selection and evaluation of internet-based information. It is therefore important that any education programme links to activities that help evaluate what is fact, what is fiction, what is opinion and whether something is plausible or biased.

In addition to accessing the internet in GHQ, children, young people and vulnerable adults may access the internet and/or use other digital technologies in their own time at other locations. This is when they will be at greater risk if they have not been taught about how to use them safely and what the dangers are.

**The Risks**

The internet is an essential element in 21st century life and ICT knowledge, now seen as an important life skill, is vital to access life-long learning and employment. While acknowledging the benefits, it is also important to recognise that risk to safety and well-being of users is ever-changing as technologies develop. These can be summarised as follows:

* **Content**
* Commercial (adverts, spam, sponsorship, personal information).
* Aggressive (violent/hateful content).
* Sexual (pornographic or unwelcome sexual content).
* Values (bias, racism, misleading info or advice)
* **Contact**
* Commercial (tracking, harvesting personal information)
* Aggressive (being bullied, harassed or stalked)
* Sexual (meeting strangers, being groomed)
* Values (self-harm, unwelcome persuasions)
* **Conduct**
* Commercial (illegal downloading, hacking, gambling, financial scams, terrorism)
* Aggressive (bullying or harassing another)
* Sexual (creating and uploading inappropriate material)
* Values (providing misleading info or advice)

Much of the material on the internet is published for an adult audience and some is unsuitable for children and young people. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere.

It is also known that adults who wish to abuse others may pose as a child/young person/peer to engage with them and attempt to meet up with them. This process is known as ***‘grooming’***and may take place over a period of months using chat rooms, social networking sites and mobile phones.

***Cyberbullying*** is bullying through the use of communication technology and can take many forms e.g. sending threatening or abusive text messages or e-mails either personally or anonymously, making insulting comments about someone on a social networking site or blog or making/sharing derogatory or embarrassing videos of someone via mobile phone or e-mail.

**E-safety Lead**

The E-safety lead at GHQ Training Ltd is: **Vicki Stacey – Training Manager**.

**Managing Incidents**

The E-safety lead will ensure that an adult follows these procedures in the event of any misuse of the internet:

**Has there been inappropriate contact?**

1. Report to GHQ Training’s e-safety lead
2. Advise the child, young person or vulnerable adult on how to terminate the communication and save all evidence.
3. Contact the parent/carer if young person is under 18 years of age.
4. Contact the police on 101
5. Log the incident
6. Identify support for the child, young person or vulnerable adult.

**Has someone been bullied?**

1. Report to GHQ Training’s e-safety lead
2. Advise the child, young person or vulnerable adult not to respond to the message
3. Refer to relevant policies including anti-bulling and equal opportunities and apple appropriate sanctions
4. Secure and preserve any evidence
5. Contact the parent/carer if the young person is under 18 years of age
6. Consider informing the police on 101, depending on the severity or repetitious nature of the offence
7. Log the incident
8. Identify support for the child, young person or vulnerable adult

**Has someone made malicious/threatening comments? (child/young person/vulnerable adult or GHQ staff/volunteer)**

1. Report to GHQ Training’s e-safety lead
2. Secure and preserve any evidence
3. In the case of offending web-based e-mails being received, capture/copy the ‘header’ info if possible
4. Inform and request that the comments are removed from the site/block the sender
5. Inform the police on 101 as appropriate
6. Log the incident
7. Identify support for the child, young person or vulnerable adult

**Has an inappropriate/illegal website been viewed?**

1. Report to GHQ Training’s e-safety lead
2. If illegal, do not log off the computer but disconnect from the electricity supply and contact the police on 101
3. Record the website address as well as the date and time of access
4. If inappropriate, refer the child/young person/vulnerable adult to the AUP that was agreed and reinforce the message
5. Decide on the appropriate sanction
6. Inform the parent/carer if the young person is under 18 years of age
7. Contact the filtering software provider to notify them of the website
8. Log the incident
9. Identify support for the child, young person or vulnerable adult

**Has an allegation been made against a member of GHQ staff/volunteer?**

All allegations should be reported to GHQ’s e-safety lead who will then look to investigate and take the appropriate action which may include contacting the police and the LSCB.

Appendix A

Online Safety Rights Charter

1. You have the right to enjoy the internet and all the fun and safe things it has to offer.
2. You have the right to keep information about you private. You only have to tell people what you really want them to know.
3. You have the right to explore the internet but remember that you cannot trust everything that you see or read on the internet.
4. You have the right to know who you are talking to on the internet. You don’t have to talk to someone if you don’t want to.
5. Remember not everyone is who they assay they are on the internet. You have the right to tell someone if you think anyone is suspicious. If you arrange to meet someone, tell a trusted adult or take a friend with you.
6. You have the right not to fill out forms or to answer questions you find on the internet.
7. You have the right not to be videoed or photographed by anyone using cameras, web cams or mobile phones.
8. You have the right not to have any videos or images of yourself put on the internet and you have the right to report it to an adult if anyone does this. (Remember that once images are posted online, they may not be able to be withdrawn).
9. You have the right not to be bullied by others on the internet and you have the right to report it to an adult if this happens.
10. If you accidently see something you shouldn’t, you have the right to tell someone and not to feel guilty about it.
11. We are all responsible for treating everyone online with respect. You should not use behaviour or language that would be offensive or upsetting to somebody else.

Appendix B

**Internet Safety Tips and Tricks**

**It is important for carers to remind any vulnerable person who uses the internet or other communication technology of the following:**

* Always explore the privacy settings of your social networking site to protect your privacy and to protect yourself from strangers (for a range of online tutorials, go to [www.kidsmart.org.uk/skills-school](http://www.kidsmart.org.uk/skills-school))
* Facebook users can download a CEOP application to their Facebook page at <http://apps.facebook.com/clickceop> which enables quick access to help at a touch of a button
* Get friends and family to have a look at your social networking site to check that you aren’t giving out too much personal information or posting inappropriate photos/films. They might see something you’ve missed
* Keep your passwords to yourself
* Respect yourself and others online
* If you are unlucky enough to have a bad experience online, report it to the service provider and tell a trusted person. You can also report to CEOP or phone 101 (police non-emergency number)
* Cyberbullying is never acceptable. If you or someone you know is targeted by bullies online, tell them to:
* Report the bully to the website/service operator
* Keep evidence of the bullying behaviour
* Resist the temptation to reply to nasty messages
* Tell a trusted person

V5\_November 2023