Online Safety Policy

RHG Consult Ltd, Harborough Innovation Centre, Market Harborough, LE16 7WB
Tel: 0345 603 9311 www.rhgconsult.co.uk Reg No: 4776603

Online Safety Policy

Introduction

RHG Consult Ltd (RHG) recognises that technology and the use of ICT equipment, which includes desktops, laptops, tablets, smart phones and smart technology (watches, fitbits etc), is part of everyday life and that it is an essential part of learning and employment.

While using this technology to access online portals is one of the fastest and most effective ways of finding information, sharing ideas, socialising, learning and working, there is also the opportunity for risks to occur.

Keeping learners safe is of the highest priority and our policy is informed by the *Keeping Children Safe in Education 2020* guidance.

This policy should be read in conjunction with our:

- Safeguarding and Safer Recruitment Policy
- PREVENT - Prevention of extremism and radicalisation policy
- Staff Handbook (for RHG staff)

The term **'staff'** refers to all full time and part employees, and associates.

The term **'learner'** refers to any person undertaking a learning programme, qualification or apprenticeship with RHG with particular reference to:

- Children and young people up to the age of 18
- Vulnerable adults (as defined in section 59 of the Safeguarding Vulnerable Groups Act 2006 and/or those persons aged 18 and over who by reason of mental or any other disability, age or illness are or may be unable to look after themselves or are or maybe unable to protect themselves against harm or exploitation)

As part of RHG's Safeguarding responsibility, we aim to protect all learners and staff against risks associated with using the internet, sharing information online, social media, emails, chat rooms and online forums, and mobile and desktop applications. This will be known as online safety.

The aim of this policy is to:

- Provide guidance on what online safety is
- Provide guidance on how staying safe online is implemented at RHG
- Identify the roles and responsibilities of the directors, staff and learners of staying safe online
- Identify the risks, impact and potential consequences of not adhering to guidance of staying safe online

Vision

Our Online Safety vision is simple:

Safe to Learn - We want our learners and staff to work thoughtfully in a safe environment.

Safe for Life - We want our learners and staff to live a safe digital life, harnessing the great opportunities which technology brings us whilst feeling empowered to make good choices to stay safe with technology.

Our strategy is guided by the **4C's**

Contact - Social networking sites, online forums and chat rooms allow one to meet new friends and share ideas with others but unfortunately not everyone is who they claim to be. Giving out personal information could make you vulnerable to exploitation, bullying or sexual aggression.

Conduct - This behaviour can be by, or towards, individuals and can include cyberbullying and cyberstalking. Behaviours can also include racism and piracy. When using equipment provided by RHG and your employer, you have a right to be protected and a duty to behave honestly and responsibly. Never do anything that makes you vulnerable to malicious software or charges of bad behaviour. Incorrect use of equipment, including downloading or passing on illegal or inappropriate content, could result in the user committing a criminal offence. The more you use the internet and social networking sites the larger your digital footprint becomes.

Content - Online content may not be suitable for learners or staff and may be hurtful or harmful. This is particularly true for content accessed and viewed via social networks, online games, blogs and websites. It's important for everyone to be aware of the reliability of online material and that it might not be true or written with a bias. There can be legal consequences for using or downloading copyrighted content, without seeking the author's permission.

Commercialism - Advertising, marketing emails and pop-ups can divert you to websites encouraging you to spend money online. There is a risk of financial abuse when making a purchase online through an unsecure source, so always check that a site belongs to the company it says it does

Online Safety Policy

In order to safeguard our staff and learners against the risks associated with online activity, RHG aims to:

- Provide all staff and learners with sufficient information regarding staying safe online and help them develop the skills to safeguard themselves.
- Work with outside agencies to develop a consistent coherent approach to safeguard learners and staff to the threat posed by having an online presence
- Involve staff, learners and employers in the review and training of online safety and raise awareness of staying safe online
- Have a Designated Safeguarding Lead who will deal with safeguarding issues including staying safe online and reporting incidents of online abuse
- Provide all staff with appropriate Safeguarding training that includes staying safe online

Responsibility
Our Designated Safeguarding Lead is and Kelly Jackson.

Our Director with responsibility for online safety is Lee Patterson.

Kelly Jackson is responsible for raising awareness of online safety and monitoring online safety through our Safeguarding procedures.

All staff are responsible for safeguarding learners and other staff and must remain vigilant at all times to support learners and colleagues to keep safe online.

The Directors of RHG are responsible for:

- Identifying and installing suitable anti-virus and anti-malware software where internet access is required for staff carrying out duties on behalf of RHG.
- Putting systems in place for monitoring responsible use of ICT equipment by staff
- Providing training for staff in online safety
- Providing resources that can be accessed by staff and learners in staying safe online
- Maintaining up to date policies and procedures for online safety

Learning coaches have the following responsibilities:

- Provide information about online safety and security related to the internet and electronic communications to all learners at induction and throughout their learning journey
- Ensure learners and all other non-employees of RHG are not given passwords and access to staff and management information systems and the internet without authorisation from the Managing Director
- Ensure learners fully understand the limits and reasons of internet searches and the use of the internet for research purposes
- Connect to the internet only through a secured network service
- Report concerns to the Designated Safeguarding Lead
- Ensure learners understand that material sourced on the internet is subject to copyright legislation and that plagiarism of material from the internet is not acceptable unless referenced within the main text or bibliography of any written assignment or evidence.
- Ensure the use of virtual meeting rooms (Zoom, Ms Teams, Webex) used for learning webinars is in accordance with best practice use and safety protocols are understood and set.

All RHG staff must:

- Never hold in their possession illegal materials/images in electronic or other format
- Never download or access illegal or indecent images or sites or anything that may bring RHG into disrepute at any time or in any place
- Ensure all communication with learners is solely for the purpose of learning, teaching and assessment and carried out in a professional manner using only an official RHG email address and RHG landline or authorised mobile phone numbers
- Never engage with any learners via contact/webcam sites (for example chat rooms, message boards and newsgroups)
- Use only RHG authorised virtual meeting rooms and webinar technology – Zoom, MS Teams and Webex and only access these sites using their RHG log-ins and passwords.
- Always seek permission from learners and other staff before recording a virtual meeting/learning session and always state the purpose of the recording.
- Never deliberately download a virus or malware or forward a link to other staff or learners that may contain a virus or malware.
- Never use the internet to harass, offend or bully any other person
- Ensure their social media accounts are used in a professional manner that will not damage RHG's brand, ethical values or bring the company into disrepute

Responsibilities of learners:

- To have a responsible attitude to the use of ICT equipment and internet/email provision
- To agree to and follow policies and guidelines on acceptable use and to report any misuse or suspected misuse by others, including bullying and harassment via electronic means
- To behave respectfully towards other learners and RHG staff when participating in virtual learning sessions and meetings
- To do all they can to keep safe online and not put themselves, RHG staff or the digital security of RHG at risk with their online behaviour

Guidance to learners
RHG staff should give timely and appropriate information to learners on internet safety which may include but is not limited to:

- Never tell anyone they meet on the internet personal details such as their home address, phone numbers, photos or bank details
- Never tell anyone they meet on the internet their employer's name or phone number
- Never arrange to meet in person someone they first met online
- Ensure they understand that not everything they read online is true

Unauthorised access
RHG staff must never give other people access to their RHG laptops, desktops or mobile devices that are used for RHG work activities. This includes other RHG staff with the exception of:

- RHG Directors
- A named IT personnel with the authorisation of the RHG Directors

Any staff allowing unauthorised access to any IT equipment supplied by RHG or used to carry out RHG work activities may face disciplinary action.

Use of email
The following procedures must be followed by all learners and staff to ensure safe and responsible use of email. It should be remembered that emails are recorded, can be traced back to the sender and can be legally binding.

- Passwords should be changed regularly and must not be shared
- Learners should adhere to their own organisation's IT and online safety policies, procedures and protocols
- Where emails are exchanged between RHG staff and learners, they should check that the email originates from the correct email address
- RHG staff and learners should not open attachments or links from an unknown source and should always check the authenticity of a link or attachment prior to clicking on it
- RHG staff must use BCC when sending out group emails to learners unless:
    - All the learners are from the same organisation and are using their organisation's email address
    - Learners and their employers have given permission to share their work email

addresses

- RHG staff should never use their RHG email accounts to send personal private or confidential information or provide personal credit card details

RHG's use of social media

At RHG we use social media and our online presence to support communication and marketing activities. We adhere to and will respond with the following:

- Restricting access to RHG social media accounts only to authorised staff
- Messages on social media relate to good news, course updates and positive achievements
- We do not engage in challenging conversations with users on social media in a public forum, but direct them to make contact directly with us using an online form, email or phone call
- We do not mention or share identifiable images of learners on social media without the authorisation of the Director with responsibility for Safeguarding
- We do not use social media to discuss religious or political issues
- We respond to any criticism in a timely and positive fashion with the outcome to demonstrate our openness, transparency and desire to work in a positive and proactive way with learners and organisations
- We regularly review our communications to ensure we act and communicate in an appropriate way for the particular social media tool - in line with our corporate image and responsibility.

Virus protection

All RHG equipment used for access to the internet is installed with anti-virus software. Introducing viruses to computers, or attempting to break through network security, is a serious offence and may result in disciplinary action or legal action being taken.

Copyright

Copyright rules apply to material available over the internet and will generally be subject to the same level of protection as material in other media. Although there are no specific exceptions from copyright material on the internet, those relating to fair dealing for the purposes of non-commercial research or private study may apply. Users should be aware of copyright notices on websites setting out how the material may be used and how to obtain permission.

Guidelines on the use of material off the internet are as follows:

- Learners and staff should acknowledge any sources within any documentation they have produced

- Users should not assume that educational use of material is permitted, without first checking with the author. Web-based resources may themselves have been published without the appropriate permissions. Therefore, any subsequent use of such material may also be illegal

- Publishing other people's material without their explicit permission is a breach of copyright. This applies to use of images from the internet used within a document

- Showing and accessing websites in a lesson is not a breach of copyright but copying an entire page without appropriate permission for own use, eg a PowerPoint presentation, is

- Copying material from the internet and printing it for pupil use could be a breach of copyright. Using it as part of a larger document without appropriate permission would be

- Copyright laws vary between countries

Website

Access to the RHG website is open to all. However, the authority to be able to add information to the website is restricted to designated staff and monitored by the Directors.

Where a picture or image of a learner, employer and or a member of staff is used, permission to use this image will be sought from the individual beforehand. Where a learner is aged below 18 or is a vulnerable adult, consent will be gained from their parents or guardians. Any image shared by RHG will be done so in a positive manner, in accordance with guidance set out in this policy.

RHG has a responsibility to protect all staff and learners and will consider the risks involved in any information which appears on our website.

Where a testimonial is attributed to an employed learner, permission from their employer will be sought beforehand with due regard being paid to any non-disclosure agreement that has been signed between the employer and RHG

Mobile phones and electronic devices

The following rules should be followed to minimise the risk of inappropriate or illegal use of these devices while learners are undertaking training and assessment with RHG:

- Learners' mobile phones must be switched off or set to silent during all training and assessment sessions unless special permission is given by their learning coach

- Inappropriate use of text messaging is not allowed at any time by staff and learners

- No photographs, video or sound recordings can be taken without the approval of the subject, whether learners or staff

- Bluetooth technology should not be used to transfer images at any time by staff or learners. Such images can be picked up by other Bluetooth enabled devices belonging to others in the area

- These rules apply to any equipment offering the same functions as mobile phones

- Incidents of intimidation and bullying with such devices will be referred to RHG's Designated Safeguarding Lead. If the incident involves a staff member, they may be subject to disciplinary proceedings

- Serious incidents of intimidation and bullying will be reported directly to the police

Disciplinary procedures

RHG will not tolerate any behaviour that places staff and learners at risk. Staff who fail to comply with this policy may be subject to disciplinary action. RHG will contact the employers (when applicable) of learners who fail to comply with this policy, and learners could face termination of their training programme. Any allegations that have justifiable evidence of criminal activity will be referred directly to the police.

If a member of staff is suspended pending investigation, permissions to use RHG ICT resources will be prohibited. Use will only be reinstated if the investigation is resolved and the member of staff is reinstated.

Signed: 

Name: Lee Patterson

Position: Managing Director

Date: 13/10/23

Date of next review: 12/10/24