E-Safety Policy

Tolley recognises it has a duty to provide students with quality internet access as part of their learning experience and that students should have an entitlement to safe internet access at all times. Tolley also recognises its obligations under Prevent Duty and employs filtering/firewall systems to prevent staff and students from accessing extremist websites and materials.

The e-safety policy extends to the full range of electronic communications including the internet, mobile phones, and wireless technology.

It is important to understand the benefits, risks, and responsibilities of using information technology. These risks include:

- Access to illegal, harmful, extremist, or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable videos/internet games

- An inability to evaluate the quality, accuracy, and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the student

Students will receive training on e-safety from their employers which will cover what kind of internet use is and is not acceptable. Students will be given clear objectives for internet use and use of other new technologies.

If a student receives an offensive or abusive email, they must immediately inform their tutor or another member of staff who will report it to the Designated Safeguarding Person.

Mobile phones must not be used in classrooms unless specifically allowed to support learning and approved by the tutor.

Virtual classrooms & staying safe online

It is important that apprentices are aware of the impact that online activity can have on other people. Apprentices should be aware of who is able to view, and potentially share, the information that is posted. Personal information should be kept safe and not shared with strangers.

Some online content may be hurtful or harmful. This is true for content accessed and viewed via social networks, online games, blogs, and websites. Apprentices should consider the reliability of online material and be aware that it may not be true or that it may have been written with a bias. Before a comment

is liked or shared online, staff should refer to the **SHARE** checklist to make sure they are not contributing to the spread of harmful content.

SOURCE: Rely on official sources for medical and safety information.

HEADLINE: Always read to the end of the article before you share, as headlines do not always tell the full story.

ANALYSE: Analyse the facts and use fact-checking services to confirm whether information is correct.

RETOUCHED: Watch out for misleading pictures and videos that might be edited or show an unrelated place or event.

ERROR: Look out for typos and other mistakes. Official information will always be carefully checked.

Consideration should be given to the fact that people online may not be who they say they are and that once someone is added to an online account, one may be inadvertently sharing personal information with them. Regularly reviewing friends lists and removing unwanted contacts is a useful action. Privacy settings online may also allow for customisation of information that each person is able to access. Inappropriate behaviour should be reported immediately.

TEN TOP TIPS FOR STAYING SAFE ONLINE

Do not post any personal information online including personal addresses, email addresses, or telephone numbers.

Think carefully before posting pictures or videos. Once a picture has been posted online many people can see it and may also be able to download it.

Keep privacy settings as high as possible.

Never share passwords.

Do not befriend strangers.

Do not meet up with people you have met online. Speak to somebody you trust if you are being pressured to take conversations offline.

Remember that not everyone online is who they say they are.

Think carefully about what you say before you post something online.

Respect other people's views.

If you see something online that makes you feel uncomfortable, unsafe, or worried: leave the website, turn off your computer/phone, and tell somebody you trust immediately.

Jonathan Scriven – Director of Tax Markets