A screenshot of a video game

Description automatically generated with medium confidence

E–Safety/ ICT/ Social Media & Online Safety Policy

Reviewed: 30 08 25– Jay Treacy/ Emily Wittering

Next review date: By 1st Sept 2026

**Uneek Learning’s e-safety policy**

Young people’s privacy is respected, their dignity encouraged and information confidentially handled. Staff and young people are kept safe and identities are protected.

Uneek Learning will take positive steps to protect the confidentiality of information stored on laptops and to prevent unauthorised access and inappropriate use.

Due to the sensitive nature of the work we undertake, we need to protect ourselves personally, as well as the company and our young people.

Uneek Learning will provide students with laptops, printers and access to the internet. These facilities will not be abused, and the young person’s welfare is paramount. Uneek Learning will ensure students are safeguarded.

**What we do**

* Take appropriate measures to eliminate unauthorised access to laptops at the time of logging on by enabling the security features available with the machine.
* Uneek Learning have two separate Wi-Fi systems – One is ‘Uneek Staff’ and the other is ‘Uneek Students’.
* The student Wi-Fi has high content/firewall restrictions that do not allow access to social networking sites, explicit content online, apps, games, you tube and other media with sensitive content via student laptops.
* The staff server which is linked to staff laptops does not allow access to any social media sites with sensitive content, although does allow access to You Tube and relevant teaching sites for lesson planning and teaching purposes.
* Students are not permitted to access staff laptops and allowing a student to do so would lead to disciplinary action.
* All student laptops at Uneek Learning have a password that staff enter to allow access to students. The passwords are kept confidentially on the staff google drive and are updated/ changed termly (or more regularly as required).
* Passwords must never be given out to students.
* Enable the computer’s screen save facility so that the screen is blanked at regular intervals which reflect the amount of passing people.
* Never leave sensitive or confidential material on their screen when the computer is unattended.
* Ensure the computer screen is not easily visible to visitors.
* All information on staff laptops to be stored on work Google Drive-not desktop.
* All student information, including referral forms, progress trackers, reports are typed directly onto Google drive and not saved onto staff laptops. Concerns and safeguarding matters are reported directly onto My Concern and not saved onto staff laptops.
* Students are always supervised when using laptops. If a staff member is required to leave a classroom and there are no other staff present in the room, the student’s work must be saved to their personal file and the laptop closed to ensure safeguarding of students.
* It is all staff responsibility to ensure laptops are logged off and closed when lessons have ended and break/ lunch times have commenced.
* The Data Protection Officer (Jay Treacy) is responsible for overall compliance and e-safety at Uneek Learning.
* The E-Safety Co-ordinator (Tom Crawley) is responsible for development of an e-safety culture at Uneek Learning and the main point of contact on day to day issues relating to e-safety and internet login support.
* The external Data Protection advisor is Nathan Drinkall- Drinkall Electrical and Security.

**Social Networking sites**

* All employees must not use a computer/ laptop to access any social networking sites during contact time with a young person or at any time during their working hours.
* All employees who use such sites out of work time are not permitted to mention any matters related to work, i.e., situations that have occurred, names of houses, names of staff members, names of young people, etc on any employee’s home page. There should be no mention of work related issues whatsoever. To do otherwise will be in breach of confidentially in addition to failure to follow to instruction.
* All employees should never accept or instigate any contact on any such sites, including emails from the young people within our education, either presently or historically. Any such attempts at making contact with you should be immediately reported to DSL’s Emily Wittering, Jay Treacy, Sonya Raybould – Secondary. DSL’s Natalie Sharpe, Stacey Bruce - Primary.

We are encouraging all employees to be very aware that such social utility sites leave individuals vulnerable to the disclosure of personal information and therefore we are reminding everyone that they should use such sites with care and attention relating to who they make contact with.

The Uneek Learning staff must ensure:

* Young people are supervised when using IT Equipment.
* Computer equipment is looked after and any faults are reported straight away.
* Computers and printers are switched off when not in use.
* Young people share the facilities and take into account the needs of others.
* Staff and young people handle the equipment gently.
* Nobody eats or drinks in close proximity to the equipment.
* Young people don’t send abusive, threatening or intimidatory e-mails or messages to anyone.
* Young people don’t download files etc... without permission.
* Young people don’t access illegal pornographic material.
* Young people don’t tamper, try to repair, or relocate any equipment.

**Teaching e-safety**

Uneek Learning’s tutors use all opportunities to discuss and advise students on safe internet use: in personal tutorials, PSHE (Well-being and Enrichment) lessons and subject lessons as appropriate.

Personal tutorials and PSHE (Well-being and Enrichment) lessons include instruction and advice on use of the internet and sites to avoid; social networking including privacy settings and keeping personal information and photographs private, awareness of grooming techniques and instructions on avoiding being drawn into meetings with strangers.

Information is also given on where to go for help and advice, regarding concerns about the internet and any communications students may receive or be involved in.

**Emergency Procedures and e-safety**

In an emergency where a staff member is called away all laptops or computers will be shut down with any work saved to the drive. If there is no time available, then as a minimum, all devices should be turned off at the main switch by a staff member only. If there is no time available, all students should be escorted out of the room and to a safe place with another staff member ( i.e. another classroom), until their return.

**Reporting e-safety issues and concerns**

Students are advised to report e-safety issues or concerns to any staff member. Staff at Uneek Learning are aware through induction and regular e-safety training that they should consult with DSL’s ( Jay Treacy/ or Emily Wittering) for e-safety safeguarding concerns and the E-safety Co-Ordinator (Tom Crawley) for any e-safety issues that require maintenance or advice.

Parents should contact the Business Manager/DSL – Emily Wittering on 01455 234611 or [emily@u-neeklearning.org](mailto:emily@u-neeklearning.org) if they have any concerns.

Staff should speak to the DSL’s about concerns as soon as possible.

**Managing e-safety issues and concerns**

This section should be read in conjunction with our Uneek Learning’s Safeguarding and Child Protection Policy and the Behaviour Policy.

The DSL’s, and if appropriate the student’s, will meet to discuss the concern and the steps that can be taken to advise and protect the student or students concerned.

The Proprietor/ Education Director (Tim Payne / Jay Treacy) will become involved if the situation is a particularly serious or difficult one.

Parents of the student or students involved will be notified and consulted and may be called into a meeting with Uneek Learning’s staff.

**Cyber-bullying**

If the on-line issue concerns bullying, the procedures and sanctions outlined in Uneek Learning’s Anti-Bullying Policy, please see these policies for more information.

**Management of personal data**

On joining Uneek Learning, students / parents sign a Learning Agreement, allowing Uneek Learning’s to use their personal data, if necessary, for on-line applications to the examination boards for access arrangements for exams, such as applications for extra time. This is usually completed with the referring school or inclusion & behaviour partnership as part of the referral process.

**Uneek Learning’s website / social media**

We sometimes use photographs of students on our website and on our Business Instagram page. Photographs of students’ creative work are also sometimes used on our website or on social media sites. All Parents and guardians are asked to give their written consent to this when students enrol at Uneek Learning.

Students are not identified by name in photographs used on the website and in the unlikely event that an individual’s name is needed, Uneek Learning would seek express permission for this each time.

**Informing and educating parents/guardians about on-line safety**

Parents and guardians are asked to read our policies on e-safety, Child Protection and Anti-bullying, which are made available on Uneek Learning’s website.

More information may be obtained from:

The UK Safer Internet Centre ([www.saferinternet.org.uk](http://www.saferinternet.org.uk)).

This Policy will be reviewed annually or sooner if Risk Assessments raise concerns.

.