

Fix-It UK Limited

IT APPROPRIATE USE POLICY

September 2023 - August 2025

The Importance of E-Safety

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Students use the Internet outside of learning and will need to learn how to evaluate Internet information and to take care of their own safety and security. Consequently, at Fix-It UK Limited we need to build in the use of these technologies in order to arm our students with the skills to access life-long learning and employment.

E-safety involves students, staff, trustees and parents making the best use of technology, information and training to create and maintain a safe online and ICT environment for Fix-It UK Limited.

Organisation / Provision

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and students, and so Fix-It UK Limited has a duty to provide students with quality Internet access as part of their learning experience:

- Fix-It UK Limited's Internet access will be designed expressly for student use including appropriate content filtering.
- Students will be given clear objectives for Internet use and taught what is acceptable use and what is not.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Fix-It UK Limited will ensure that the use of Internet derived materials by staff and students complies with copyright law.

Through ICT, we ensure that Fix-It UK Limited meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that we meet the diverse needs of students to ensure inclusion for all and that all students are prepared for full participation in a multi- ethnic society. Students are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.

Reporting

All breaches of the e-safety policy need to be recorded, the details of the user, date and nature of incident should be recorded.

Incidents which may lead to child protection issues need to be passed on to one of the Designated Safeguarding Leads immediately. Incidents which are not child protection issues but may require intervention (e.g. cyberbullying) should still be reported to the Safeguarding Lead on the same day of the incident. Evidence of incidents must be preserved and retained.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act.

Assessing Risk

Fix-It UK Limited will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer at Fix-It UK Limited. Fix-It UK Limited does not accept liability for the material accessed, or any consequences of Internet access. Fix-It UK Limited will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to management.
- Complaints of a child protection nature shall be dealt with in accordance with Fix-It UK Limited's child protection procedures.
- Students and parents will be informed of the complaints procedure.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Internet

Whilst ICT is exciting and beneficial in and out of education, web based resources are not well policed. All users need to be aware of the range of risks associated with the use of these internet technologies and their individual responsibilities relating to the safeguarding of children and themselves.

Educating students on the dangers of technologies that maybe encountered is done informally when opportunities arise and as part of E-safety. Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying.

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children:

Learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or students discover unsuitable sites, the URL (address), time and content shall be reported to staff who will then report to management, by recording the incident in an e-Safety Log, which will be stored in the Main Office with other safeguarding materials. The e-Safety Log will be reviewed termly.
- Fix-It UK Limited will ensure that the use of Internet derived materials by staff and students complies with copyright law.
- Students will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Managing the Internet

- Fix-It UK Limited maintains that students will have supervised access to Internet resources through fixed and mobile internet technology. All staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with students.
- All users must observe software copyright at all times. It is illegal to copy or distribute Fix-It UK Limited owned software or illegal software from other sources. All users must observe the copyright of materials from electronic resources.

Authorised Internet Access

By explicitly authorising the use of Fix-It UK Limited's Internet access students and staff are provided with information relating to e-safety and agree to its use:

- Only authorised equipment, software and Internet access can be used within the learning environment.

Security

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Students and staff should never share passwords and staff must **never** let students use a staff logon. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

Password security

- Password security is essential for everyone.
- Students are expected to keep their passwords secret and not to share with others, particularly their friends.
- Staff and students are regularly reminded of the need for password security.

Software security

- A security breach, lost stolen equipment, virus notifications, unsolicited emails and all other policy non-compliance must be reported to senior management.
- To minimise risk, students should not bring portable memory sticks into the building.

Information System Security

- Fix-It UK Limited ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- E-safety will be discussed with our ICT support and those arrangements incorporated into our agreement with them.

E-mail

- Students must immediately tell a member of staff / trusted adult if they receive an offensive email.
- E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:
- Students must immediately tell a member of staff if they receive an offensive email.
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- E-mail sent to external organisations should be written carefully and authorised before sending.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Social Networking

- Social networking Internet sites (such as Twitter, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.
- Use of social networking sites and newsgroups in Fix-It UK Limited, is not allowed and will be blocked/filtered.
- Students will be advised never to give out personal details of any kind that may identify themselves, other students, their school or location. This will also include not using personal photographs and videos.
- Students will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Students and staff will be advised of the dangers of discussing students, staff or Fix-It UK Limited on social networking sites. Legal action will be considered, where appropriate, to protect students and staff against cyberbullying and defamatory comments.

Mobile Phones

Mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Students by permission of senior management can bring mobile phones on site where it is seen by Fix-It UK Limited as a safety/precautionary use.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff should always use the reception/office phone to contact parents/guardians/care providers.
- Staff, including students and visitors, are not permitted to access or use their mobile phones within a learning environment. All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the teaching day.
- Staff may use their mobile phones in the main office/reception, out of sight of students.
- On trips staff mobiles are used for emergencies only.

Communication of Policy

Students:

- Rules for Internet access will be posted in all networked rooms.
- Students will be informed that Internet use will be monitored.
- Students will be informed of the importance of being safe on social networking sites such as Facebook. This will be strongly reinforced.

Further Resources

We have found these websites useful for e-safety advice and information.

<http://www.thinkuknow.co.uk/>

Set up by the Police with lots of information for parents and staff including a place to report abuse.

<http://www.childnet-int.org/>

Non-profit organisation working with others to “help make the Internet a great and safe place for children”.