EDUCATION EDIT

Unit 2, BizSpace
Planetary Road
Willenhall, WV13 3SW

www.editeducation.co.uk
contact@editeducation.co.uk
07850 444 238

ONLINE SAFETY POLICY
September 2024

Policy Review

This policy will be reviewed in full by the Directors on an annual basis unless circumstances require policy update in the interim.

The policy was last reviewed and agreed by the Directors on 01.09.24.

It is due for review on 01.09.25 (up to 12 months from the above date).

AM.Nangreen

Signature (CEO) ……………………………. Date ……01.09.24………………

Bentley

Signature (COO) …………………….………   Date …….01.09.24………………

Version Control

Version	Date	Changes
V1	04/09/23	Original document
V2	01/09/24	Terminology and layout update

1. Rationale

It is the duty of Edit Education to ensure that every student in their care is safe, and the same principles should apply to the ‘virtual’ or digital world as would be applied to the real world. Increasingly, students are accessing material through the internet and games consoles which is not age appropriate. It is essential to address this and to encourage a lifestyle which incorporates a healthy balance of time spent using technology.

This policy for staff, directors, visitors and students, is to protect the interests and safety of the whole provision community and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. It is linked to the following provision policies: Child Protection, Health and Safety and Behaviour.

Both this policy and the Acceptable Use Policies (for all staff, directors, visitors and students) are inclusive of both fixed and mobile internet, technologies provided by the provision (such as PCs, laptops, whiteboards, tablet, voting systems, digital video and camera equipment, etc) and technologies owned by students or staff.

2. The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information.

Current and emerging technologies used in provision and, more importantly in many cases, used outside of provision by children include:

- The Internet
- e-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat Rooms
- Gaming Sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as Smart Phone and Tablets.

3. Whole Provision Approach to the Safe use of ICT

Creating a safe ICT learning environment includes three main elements in Edit Education:

1. An effective range of technological tools which are filtered and monitored.

2. Policies and procedures, with clear roles and responsibilities.

3. A comprehensive e-Safety education programme for students, staff and parents.

Staff Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in Edit Education and the CEO aims to embed safe practices into the culture of the provision. The CEO ensures that the policy is implemented and compliance with the policy monitored. All staff are encouraged to create a talking culture to address any e-safety issues which may arise in classrooms on a daily basis.

The responsibility for e-Safety has been designated to a member of the provision leadership team.

Our provision e-Safety lead is Alex Nangreave.

Our e-Safety lead ensures he keeps up to date with e-Safety issues and guidance through organisations such as The Child Exploitation and Online Protection (CEOP). The provision's e-Safety lead ensures the COO, Senior Management and directors are updated as necessary.

4. Staff awareness

All staff receive regular information and training on e-safety issues in the form of in house training and meeting time.

- New staff receive information on the provision's acceptable use policy (AUP) as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the provision community.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas and through a culture of talking about issues as they arise.
- E-safety records of concern are completed by staff as soon as incidents occur and are reported directly to the provision's designated safeguarding team.

All staff working with students are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following provision e-Safety procedures. These behaviours are summarised in the AUPs which must be signed and returned before use of technologies in provision.

5. Internet:

- The provision will use a "filtered" Internet Service, which will minimise the chances of students encountering undesirable material.

- Staff, students and visitors have access to the internet through the provision's fixed and mobile internet technology.

- Staff should email provision-related information using their provision account and not their personal accounts.

- Staff will preview any websites before recommending to students.

- Internet searches are conducted using the Safe Search homepage found athttp://www.safesearchkids.com/.

- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.

- If staff or students discover an unsuitable site, the screen must be switched off immediately and the incident reported to the e-safety lead detailing the device and username.

- Staff and students are aware that provision based email and internet activity is monitored and can be explored further if required.

- Students using the World Wide Web are expected not to deliberately seek out offensive materials. Should any students encounter any such material accidentally, they are expected to report it immediately to a teacher who will notify the E-safety lead.

- Students are expected not to use any rude or offensive language in their email communications and contact only people they know or those the teacher has approved.

- They are taught the rules of etiquette in email and are expected to follow them.

- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved provision project.

- Students consistently choosing not to comply with these expectations will be warned, and subsequently, may be sanctioned following the provision’s behaviour policy.

- Students will be asked to sign to the Acceptable Use Agreement thus ensuring that they are aware of expectations. Copies of the agreement will also be distributed to parents to ensure that key messages are reinforced at home.

Passwords:

- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers).

- Passwords should not be written down.

- Passwords should not be shared with other children or staff.

Mobile technology (laptops, iPads, netbooks, etc):

- Staff laptops should not be left in cars. If this is unavoidable, it should be temporarily locked out of sight in the boot.

- Staff should only use the laptop which is allocated to them.

- Mobile technology for student use, such as iPads and netbooks, are stored in a locked cupboard. Access is available via the provision office or keyholders.

Members of provision staff (not visitors or children) should sign in/out the technologies before and after each use.

- Mobile Technology assigned to a member of staff as part of their role and responsibility must have a passcode or device lock so unauthorised people cannot access the content.

- Personal devices must not be used to take pictures or videos of students

- When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

- No personal devices belonging to staff or students are to be used during learning time. If staff bring in their own devices such as mobile phones, these are to be used during break times only and kept on silent. If students bring in mobile phones (for the purpose of safety if they walk to and from provision alone), they should be kept switched off or put on silent during learning time. They will remain the responsibility of the student in case of loss or damage. Any student not following these rules will be dealt with using the provision’s behaviour policy.

Data storage

- Staff are expected to save all data relating to their work to their Laptop if they have been assigned one or to the Google Drive Account.

- The provision discourages the use of removable media however if they are used we expect the Encryption of all removable media (USB pen drives, CDs, portable drives) taken outside provision or sent by post or courier.

- Staff laptops should be encrypted if any data or passwords are stored on them.

- IEPs, assessment records, student medical information and any other data related to students or staff should not be stored on personal memory sticks.

- Only take offsite information you are authorised to and only when it is necessary and required in order to fulfil your role. If you are unsure speak to a member of the Provision Management Team.

Social Networking Sites

- Use such sites with extreme caution, being aware of the nature of what you are publishing on-line in relation to your professional position. Do not publish any information online which you would not want your employer to see.

- Under no circumstances should students or parents, past or present, be added as friends, unless known to you as a friend or relative prior to your appointment.

- Your role in Edit Education requires a high degree of professionalism and confidentiality.

- Any communications or content you publish that causes damage to Edit Education, partner organisations any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the Edit Education Dismissal and Disciplinary Policies apply. This could also undermine any complaints procedures.

- Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.

- Edit Education expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Any communications made in a professional capacity through social media must not be done either knowingly or recklessly:

- place a child or young person at risk of harm;

- bring Edit Education into disrepute;

- breach confidentiality;

- breach copyright;

- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example

by:

  - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
  - using social media to bully another individual; or
  - posting images that are discriminatory or offensive or links to such
  - content.

Edit Education reserves the right to monitor staff internet usage. The Service considers that valid reasons for checking internet usage include concerns that social media/internet sites have been accessed in breach of this Policy.

Digital images

• Use only digital cameras and video cameras provided by the provision and under no circumstances use personal equipment such as digital cameras or camera phones to store images of children unless prior authorisation has been provided.

If it is used in this way then images must be removed before leaving the provision premises.

• Ensure you are aware of the students whose parents/guardians have not given permission for their child's image to be used in provision. An up to date list is kept in the provision's referral folder in the administrative office.

• When using student's images for any provision activity, they should not be identified by their name.

Members of staff who breach the acceptable use policy may face disciplinary action. A misuse or breach of this policy could also result in criminal or civil actions being brought against you.

Providing a comprehensive E-safety education to students and parents

• All staff working with children must share a collective responsibility to provide e-safety education to students and to promote e-safety in their own actions.

• Formally, an e-safety education is provided by the objectives contained in the ICT unit plans for every area of work for each year group. Even if e- safety is not relevant to the area of ICT being taught, it is important to have this as a 'constant' in the ICT curriculum.

• Informally, a talking culture is encouraged in classrooms which allows e-safety issues to be addressed as and when they arise.

• The ICT lead will lead regular e-safety events, including on Safer Internet Day, highlighting relevant e-safety issues and promoting safe use of technologies.

• E-safety themes are also woven into the fabric of the Edit Education curriculum.

• When children use provision computers, staff should make sure children are fully aware of the agreement they are making to follow the provision's ICT guidelines.

Maintaining the security of the provision IT Network

Edit Education maintain the security of the provision network and is responsible for ensuring that virus protection is up to date at all times. However, it is also the responsibility of the IT users to uphold the security and integrity of the network Complaints procedure.

As with other areas of the provision, if a member of staff, a child or a parent / carer has a complaint or concern relating to e-safety then they will be considered and prompt action will be taken. Complaints should be addressed to the e-safety lead in the first instance, who will undertake an immediate investigation and liaise with the leadership team and those members directly involved. Incidents of e-safety concern will be recorded using a Notice of Concern proforma and reported to the provision's designated safeguarding lead in accordance with provision's child protection policy. Complaints of Cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

Monitoring

The CEO/COO or other authorised members of staff may inspect or monitor any ICT equipment owned or leased by the provision at any time without prior notice.

Monitoring includes: intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, email, texts or image) involving employees without consent, to the extent permitted by law. This may be to confirm or obtain provision business related information; to confirm or investigate compliance with Edit Education policies, standards and procedures, to ensure the effective operation of provision ICT, for quality control or training purposes, to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

Breaches of Policy

Any policy breaches are grounds for disciplinary action in accordance with the Edit Education Disciplinary Policy. Policy breaches may also lead to criminal or civil proceedings.

Incident Report

All security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the provision's Designated Safeguarding Lead