(ICT) E- Safety Policy

Date: **August 2025**

Review Date: **August 2026**

Authority: Director, Connect2Education Ltd

1. Introduction

With the increase in technology available to young people and staff, both inside and outside of Connect2Education Ltd , there is a recognised need to ensure the technologies are being used responsibly, appropriately and safely. This policy outlines training and expectations for the use of technology by all members of the organisation and potential dangers of the use of technology including outside of the Connect2Education Ltd environment.

This policy has been written in line with local and national guidance about e-safety and considers the potential for incidents of misuse or abuse of technology, some of which may be deemed acts of criminality. Connect2Education Ltd and employees recognise that some children and young people have an increased risk of abuse both online and offline.

This policy has been updated in line with changes to Keeping Children Safe in Education 2025. This policy will refer to E Safety and includes the generic term ICT (Information and Communication Technology)

2. Purpose of the policy:

This policy applies to all members of the organisation, including young people, parents/carers and staff. The policy aims to provide the following information:

- The acceptable use of technologies within Connect2Education Ltd & categories of risk .
- E-Safety via Teaching and Learning
- How we manage internet Access

- Parents and carers roles and responsibilities in promoting e-safety.
- Staff roles and responsibilities in promoting e-safety.

3. Definition of ICT Safety

E-Safety relates to the safe and responsible use of information communication technology (ICT). This includes computers, the internet, mobile communication devices and technology tools that are designed to hold, share, or receive information (for example mobile phones, digital cameras and pagers).

4. The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, misinformation, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

5. To meet our aims and address the risks above, we will:

- Educate pupils about online safety as part of our PSHE offer. For example: the safe use of social media, the internet and technology (including Artificial Intelligence)
- Keeping personal information private
- Recognise unacceptable behaviour online
- Encourage reporting of cyber bullying, including where children and young people are a witness rather than a victim
- Train staff, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying, the risks of online radicalisation, and the expectations, roles and responsibilities around filtering and monitoring. All staff members will receive refresher training as required and at least once each academic year
- Educate parents/carers about online specifically when we are working online with children and young people. We will also share clear policies and procedures, so they understand how we safeguard children and young people we work with and how to report online harms.

We will ensure that all staff are aware of any restrictions placed on them with regards to the use of their mobile phone and cameras, for example that:

- Staff are allowed to bring their personal phones to work as part of our staff tracking requirement whilst out in homes and schools but will limit such use to work requirements of checking in and out with head office and recording attendance.
- Staff will not take pictures or recordings of pupils on their personal phones or cameras
- Staff will explain the policy to pupils regarding acceptable use of the internet and mobile phones whilst in centre both on induction and during lessons if applicable.
- Put in place robust filtering and monitoring systems to limit children's exposure to the 4 key categories of risk (described above) whilst working with staff.
- Carry out an annual review of our approach to online safety.
- Provide regular safeguarding and children protection updates including online safety to all staff, at least annually, in order to continue to provide them with the relevant skills and knowledge to safeguard effectively
- Review the child protection and safeguarding policy, including online safety, annually and ensure the procedures and implementation are updated and reviewed regularly

6. The acceptable use of information and communication technology in Connect2Education Ltd.

We recognise that technology plays an important role in the education of young people at Connect2Education Ltd. Equipment such as computers, digital cameras and recording equipment offer a wide range of opportunities for the development of skills and this technology, when used appropriately, will enhance the learning process offered to young people and staff alike. Use of such technology, including the internet, is a privilege and not a right. This right is available to those who abide by the rules and always demonstrate a responsible and appropriate manner, in their use of technology. Internet access is widely available across our sites and is strictly monitored and filtered to ensure the context displayed is appropriate to the age of the young person.

7. Teaching and Learning.

Connect2Education Ltd takes the welfare of its students and staff seriously and recognises that protecting everyone from potential harm has become a wider issue than merely addressing the physical dangers presented in the world around us. The safety, both physical and on-line and emotional wellbeing of all members of Connect2Education Ltd, are paramount and considered in all aspects of teaching and learning.

8. Managing internet Access - the use of technology by staff and students in centre.

Within Connect2Education Ltd, access to the internet is offered purely as a tool for teaching and learning. Therefore, young people and staff may have monitored access to the internet only when appropriate to education-based activities.

Young people must only access the internet when given permission by a member of staff and only for educational activities, such as researching a project, or downloading information. Misuse of the internet may result in suspension from use of in-centre computers. Connect2Education Ltd monitors and filters access to content, aiming to mitigate accidental contact with material that is age inappropriate. To ensure

that children and young people are protected, a member of staff will sit side by side with the young person who is using the internet.

Access to the internet is not provided for the use of private and personal email accounts, instant messaging accounts or other forms of personal contact or entertainment.

9. Publishing Images

Images of young people must not be uploaded to the internet or website. There may be times when we update our website and may request images are used of our work in the centre. For marketing purposes, we use models not actual students. All images must be appropriate and necessary. Under no circumstances should members of staff display images of children or young people who attend the centre on their personal social networking sites, or similar personal online websites or pages. Similarly, children and young people should under no circumstances, record members of staff either on video or voice recording. take photographs of staff members on their personal cameras or electronic communication devices, such as mobile phones, nor should they upload images to the internet or forward them onwards electronically.

10. Mobile Phones

Under no circumstances should personal mobile phones be given to young people for their use e.g., to make an emergency phone call. In these circumstances young people should be referred to the senior member of staff in charge.

Young people are requested not to use mobile phones or other related communication devices whilst in lessons on the Connect2Education Ltd premises. We would like to encourage parents and carers not to send mobile phones or similar equipment with young people onto the premises. Connect2Education Ltd cannot be held responsible for any loss or damages.

11. Digital Cameras

Under no circumstances should members of staff use their own cameras, including mobile phone cameras, to take images of young people. There are times when we do take photographs of artwork or catering products connected to specific awards – this is agreed with the Principal Director prior to taking photograph of work.

12. Game Consoles

Games consoles are not permitted to be brought to our centre and Connect2Education takes no responsibility for the loss, or theft of such items. We strongly advise parents and carers to discourage their children from bringing such items on to Connect2Education grounds. Staff are also discouraged from bringing in personal technological equipment.

13. Cyber Bullying

Cyber bullying is the repeated harassment, degradation, or abuse of another, though, or with technology. There are several forms of cyber bullying, including (but not exclusively) those that take place via:

- Text message
- Phone call
- Picture/videos including those created with A.I.
- Email

- Online chat rooms
- Social networking sites
- Via websites in general (e.g., hate or bashing websites)

13. Incidents of E Safety Abuse

Connect2Education Ltd takes all incidents of misuse of technology and bullying, including cyber bullying, very seriously. All members of staff and students have a clear role to play in reporting such incidents to the office manager and to work with us to ensure such incidents are not repeated.

14. Responsibilities and Reporting Incidents – Young people & their parents/carers.

Parents and carers play an important role in developing children's understanding and awareness of e-safety by supporting Connect2Education Ltd in its endeavours to build young people's knowledge of how to stay safe when using technology. Parents and carers have a duty to report any incidents affecting young people and their education to Connect2Education to ensure that matters are investigated and dealt with swiftly.

A young person or parent/carer who is concerned about an act of misuse or abuse of technology at Connect2Education Ltd, should report the incident immediately to a member of staff.

Some incidents of misuse or abuse may be deemed a criminal offence or be of such a highly serious nature that immediate police involvement is required. In such cases, parents should contact their local police.

15. Responsibilities and reporting Incidents -Staff.

All members of staff have a duty to report any incidents of misuse or abuse of technology to a member of the Senior Leadership Team. Where staff members are the victims of abuse of technology, including harassment or cyberbullying, they should save all evidence and present it immediately to a member of the Senior Leadership Team. For serious incidents staff should contact the police, at their discretion.

Members of staff at Connect2Education Ltd have a clear and important role to play in the promotion of e-safety and should always encourage sensible behaviour from all young people, when using technology.

16. Monitoring, evaluation, and review of this policy

Given the changing nature of technology within the education environment and the wider world, this policy will be reviewed annually, with sporadic reviews, when necessary, such as in the event of new technology being utilised as a teaching and learning tool.

The Director, in conjunction with the Senior Leadership Team, are responsible for the ongoing monitoring and evaluation of this policy.

17. Policy Acknowledgement and Sign-Off

This policy must be read and signed by all staff during induction or to acknowledge policy updates.