E-Safety Policy

Rationale

Being online is an integral part of many learners' lives. Social media, online games, websites, and apps can be accessed through mobile phones, computers, laptops, and tablets – all of which form a part of young people's online world. The internet and online technology provide new opportunities for young people's learning and growth, but it can also expose them to new types of risks. E-safety forms a fundamental part of Green Corridor's safeguarding procedures

Aims

- To ensure that Learner have the opportunity to learn how to keep themselves safe when using ICT equipment, the internet and social media.
- To protect anybody who receives Green Corridor's services and who make use of information technology (such as smart phones, tablets, games consoles and the Internet) as part of their involvement with us.
- To provide staff and volunteers with the overarching principals that guide our approach to e-safety.
- To ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use information technology.

Objectives

We recognise that:

- The welfare of the Learners who come into contact with our services is paramount and should govern our approach to the use and management of electronic communication technologies.
- As adults, all Learners have the right to carry a mobile phone in Green Corridor and they should be taught to store and use them at appropriate times. Mobile phones may also be used as a learning resource to enable Learners to become more independent and access the community.
- All Learners, regardless of age, disability, gender, racial heritage, religious belief, sexual orientation, or identity, have the right to equal protection from all types of harm or abuse
- Working in partnership with Learners, their parents, carers, and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to e-safety
- The use of information technology is an essential part of our lives; it is part of how we as an organisation gather and store information, as well as how we communicate with each other. It is also an intrinsic part of the experience of our Learners and is beneficial to all. However, it can present challenges in terms of how we use it responsibly and, if misused either by an adult or a young person, can be actually or potentially harmful to them.

Teaching and Learning

The internet is an essential element for education, business, and social interaction. Internet use is a necessary tool for staff and Learners, and so Green Corridor has a duty to provide Learners with quality internet access as part of their learning experience:
Green Corridor's internet access is designed for Learner's use including appropriate content filtering, which is put in place by our IT supplier. Learners will be given clear objectives for internet use and taught what use is acceptable and what is not. The internet opens up new opportunities and is becoming an essential part of the everyday world for young people. However, there are inappropriate and undesirable elements that must be managed:

- If staff or Learner discover unsuitable sites, the URL, time, and content shall be reported to the IT provider, the DSL and the line manager of the person making the discovery.
- Green Corridor will work with its technical support provider (ITDD ltd) to ensure filtering systems are as effective as possible. We have in place web-filtering that blocks access to social media sites, chat rooms, online gaming sites and certain video hosting websites that do not have an internal filtering system.

Mobile Phones

Many 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. Learners can bring mobile phones/iPads onto the Green Corridor site, but they may not be connected to Green Corridor's IT network. The sending of abusive or inappropriate text message or photographs is forbidden. The Green Corridor reserve the right to restrict a Learner's access to their mobile phone if it poses a risk to the safeguarding of their peers.

Some staff are provided with mobile telephones to perform their duties and these phones are permitted on site. Other phones must be stored in the staff room and staff are not permitted to access them except in designated staff only areas.

Cyber Bullying

Online bullying and harassment via Instant messaging, mobile phone texting, e-mail, photos and chat rooms are potential problems that can have a serious effect on learners both in and outside Green Corridor. The methods and the audience are broader than traditional bullying and the perceived anonymity can make escalation and unintended involvement an increased risk.

Learners are taught how to use the Internet safely within our ICT curriculum. Learners are given access to guidance and support resources from a variety of sources. Specific education and training for staff on cyber bullying (understanding what behaviour constitutes cyberbullying and its impact, how to handle concerns and report incidents) is given as part induction training.
Learners are encouraged to discuss any concerns or worries they have about online bullying and harassment with their teachers. Complaints of cyber bullying are dealt with in accordance with our safeguarding Policy.

Promoting E-Safety

We are:

- Supporting and encouraging young people within the Green Corridor to use opportunities offered by mobile phone technology and the internet in ways that keep themselves safe and shows respect for others.
- Planning and delivering a curriculum that promotes maintaining safety and privacy when online or using social media, recognising danger and how to get support if needed.
- Supporting and encouraging parents and carers to do what they can to keep their young people safe online and when using their mobile phone, iPod, tablet, and game consoles.
- Incorporating statements about safe and appropriate ICT use into the codes of conduct both for staff and volunteers and for learners.
- Developing an e-safety agreement for use with young people and their carers signed during the learner's induction.
- Using our procedures to deal firmly, fairly, and decisively with any examples of inappropriate ICT use, complaints or allegations, whether by an adult or a Learner (these may include breaches of filtering, illegal use, cyber bullying, or use of ICT to groom a Learner or perpetrate abuse).
- Informing parents and carers of incidents of concern as appropriate.
- Reviewing and updating the security of our information systems regularly.
- Providing adequate physical security for ICT equipment.
- Ensuring that usernames, logins, and passwords are used effectively.
- Using only official email accounts provided via the organisation and monitoring these as necessary.
- Ensuring that images of Learners are used only after their permission where they are able to give it, and/ or parents and carers written permission has been obtained, and only for the purpose for which consent has been given.
- Any social media tools used in the course of our work with Learners and families will be risk assessed in advance by the member of staff wishing to use them.
- providing effective management for staff and volunteers on ICT issues, through supervision, support, and training; examining and risk assessing any emerging new technologies before they are used within the organisation.
- CPD to inform staff of e-safety risks, how to spot and how to report concerns.

Guidance from KCSIE

The following resources may also help Green Corridor understand and teach about safeguarding:

- DfE advice for schools: teaching online safety in schools
- UK Council for Internet Safety (UKCIS)37 guidance: Education for a connected world
- UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people
- The UKCIS external visitors guidance will help schools and Green Corridors to ensure the maximum impact of any online safety sessions delivered by external visitors
- National Crime Agency's CEOP education programme: Thinkuknow

- Public Health England38: Every Mind Matters
- Harmful online challenges and online hoaxes - this includes advice on preparing for any online challenges and hoaxes, sharing information with parents and carers and where to get help and support.

The Four C's

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas (the four C's) of risk:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, 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:** online behaviour that increases the likelihood of, or causes, harm; for example, 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. If you feel your learners or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Links with other policies

This E-Safety statement is linked to the safeguarding, IT and Disciplinary Policy.

Document Control

Person Responsible	Head of Education
Date of Policy	August 2023
Next review date	August 2026
Version	1.0
Author	David Welch
1st Approval	Ruth Kennedy
2nd Approval	Nicola Jennings