Great Oaks College Great Oaks College E Safety Policy	
Person Responsible:	Richard Murr – Deputy Principal, Designated Safeguarding Lead, Oversite of IT
Date of Policy:	September 2022
Next review date:	September 2023

Rationale

Being online is an integral part of young people's 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 provides 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 colleges' safeguarding procedures

Aims

- To ensure that student have the opportunity to learn how to keep themselves safe when using ICT equipment, the internet and social media.
- To protect anybody who receives Great Oaks Colleges services and who make use of information technology (such as smart phones, iPods, iPads, 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 students 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 students have the right to carry a mobile phone in college and they should be taught to store and use them at appropriate times. The college provide purpose built lockers for phones/devices to be stored and charged safely. Mobile phones will also be used as a learning resource to enable students to become more independent and access the community.
- All students, 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 students, 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 students, 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 students, and so the college has a duty to provide students with quality internet access as part of their learning experience:

The college internet access is designed for student's use including appropriate content filtering. Students 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 student discover unsuitable sites, the URL, time and content shall be reported to the ICT Helpdesk who will then record the incident. The e-safety log will be reviewed termly by the DSL.
The college will work with its technical support provider (LGFL) to ensure filtering systems are 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 new 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 the Deputy Principals can bring mobile phones onto the college site. As appropriate, students will either leave these in the college office or store them in the provided phone locker. Vocational students may only use their phones in the common room, link bridge and the Ok Café during break times. The sending of abusive or inappropriate text message is forbidden. The college reserve the right to restrict a student's access to their mobile phone if it poses a risk to the safeguarding of their peers.
Staff and visitors, are not permitted to access or use their mobile phones within the college apart from designated staff only areas.

Cyber Bullying
Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on students both in and outside college. The methods and the audience are broader than traditional bullying and the perceived anonymity can make escalation and unintended involvement an increased risk.
Students are taught how to use the Internet safely within our ICT curriculum. Students 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.
Students 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-Saftey

- Developing a range of procedures that provide clear and specific directions to staff and volunteers on the appropriate use of ICT; this is available within the staff code of conduct and the staff handbook.
- Supporting and encouraging young people within the college 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 students;
- Developing an e-safety agreement for use with young people and their carers; (Annex 1)
- Use our procedures to deal firmly, fairly and decisively with any examples of inappropriate ICT use, complaints or allegations, whether by an adult or a student (these may include breaches of filtering, illegal use, cyber bullying, or use of ICT to groom a student 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 user names, logins and passwords are used effectively;
- Using only official email accounts provided via the organisation, and monitoring these as necessary;
- Ensuring that the personal information of staff, volunteers and service users (including service users' names) are not published on our website;
- Ensuring that images of students 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 students and families must 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 hot to report concerns.

Guidance from KCSIE

The following resources, may also help colleges 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 colleges 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 pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Annex 1

Great Oaks College Online safety agreement

Parents/carers: please read and discuss this agreement with your young person and then sign it, ask your young person to sign it, and return it to the college. If you have any questions or concerns please speak to

Richard Murr – Deputy Principal.

Young person's agreement

¯ I will be responsible for my behaviour when using the internet, including social media platforms, games and apps. This includes the resources I access and the language I use.

¯ I will not deliberately browse, download or upload material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to the teacher.

¯ I will not send anyone material that could be considered threatening, bullying, offensive or illegal.

¯ I will not give out any personal information online, such as my name, phone number or address.

¯ I will not reveal my passwords to anyone.

¯ I will not arrange a face-to-face meeting with someone I meet online unless I have discussed this with my parents/Carers and am accompanied by a trusted person.

¯ If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I can talk to Rich Murr

I understand that my internet use at Great Oaks College will be monitored and logged. I understand that these rules are designed to keep me safe and that if I choose not to follow them, Great Oaks College may contact my parents/carers/Social Worker.

Signatures:

We have discussed this online safety agreement and _____ agrees to follow the rules set out above.

Parent/carer signature……

Date ……

Young person's signature……
Date ……..