E- safety/Internet Safety Policy

Important terms used in this document:

- *The abbreviation 'ICT' in this document refers to the term 'Information and Communication Technologies.*
- *'Cyber safety' refers to the safe and responsible use of the Internet and ICT equipment/devices, including mobile phones*
- *'The CTSA 2015' Counter Terrorism and Security Act*
- *(KCSIE) refers to Keeping children safe in Education*
- *'School ICT' refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below*

The term 'ICT equipment/devices' used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players),Gaming Consoles, and any other, similar, technologies as they come into use.

Policy on Internet (Cyber) Safety

Rationale

FreshSteps has a statutory obligation to maintain a safe physical and emotional environment, and a responsibility to consult with the community. In addition FreshSteps has a responsibility to be a good employer.

These three responsibilities are increasingly being linked to the use of the Internet and Information Communication Technologies (ICT), and a number of related cyber safety issues. The Internet and ICT devices/equipment bring great benefits to the teaching and learning programmes, and to the effective operation of the school.

FreshSteps places a high priority on providing the school with Internet facilities and ICT devices / equipment which will benefit student learning outcomes, and the effective operation of the school.

However, the school recognises that the presence in the learning environment of these technologies (Some provided partly or wholly by the school and some privately owned by staff, students and other members of the school community), can also facilitate anti-social, inappropriate, and even illegal, material and activities. The school has the dual responsibility to maximise the benefits of these technologies, while at the same time to minimise and manage the risks.

The School thus acknowledges the need to have in place rigorous and effective school cyber safety practices which are directed and guided by this cyber safety policy.

E-Safety

When using technology our filtering and password protected system ensures that our students are safe from terrorist and extremist materials when accessing the internet.

FreshSteps fully endorse the CTSA 2015 Act **PREVENT** duty strategy that:

Schools can help to protect children from extremist and violent views in the same ways that they help to safeguard children from drugs, gang violence or alcohol. Their purpose must be to protect children from harm and to ensure that they are taught in a way that is consistent with the law and our **values.**

FreshSteps has followed guidelines from DFE with regards to KCSIE to ensure we have a regard to it when carrying out our duties to safeguard and promote the welfare of all our students.

All staff will be trained to notice possible behaviour changes in any student thus identifying students who might be at risk radicalisation.

FreshSteps will develop and maintain rigorous and effective cyber safety practices which aim to maximise the benefits of the Internet and ICT devices/equipment to student learning and to the effective operation of the school, while minimising and managing any risks.

These cyber safety practices will aim to not only maintain a cyber safe school environment, but also aim to address the need of students and other members of the school community to receive education about the safe and responsible use of present and developing information and communication technologies.

Policy Guidelines

Associated issues the school will address include: the need for on-going funding for cyber safety practices through inclusion in the annual budget, the review of the school's annual and strategic plan, the deployment of staff, professional development and training, implications for the design and delivery of the curriculum, the need for relevant education about cyber safety for the school community, disciplinary responses appropriate to breaches of cyber safety, the availability of appropriate pastoral support, and potential employment issues.

To develop a cyber safe school environment, the board will delegate to the principal the responsibility to achieve this goal by developing and implementing the appropriate management procedures, practices, electronic systems, and educational programmes. A process for reporting back to the board by the principal will be agreed upon and established. Frequency and content of reporting will be included.

In recognition of its guardianship and governance role in the cyber safety of the school, the board will also develop a policy relating to board governor's use of ICT devices / equipment. This will cover all use of school-owned/leased and privately owned/leased ICT devices/equipment containing school data/information on or off the school site.

Guidelines for FreshSteps Cyber Safety Practices

1. No individual may use the school Internet facilities and school-owned ICT devices/equipment in any circumstances unless the appropriate use agreement has been signed and returned to the school. Use agreements also apply to the use of privately-owned/leased ICT devices/equipment on the school site, or at/for any school-related activity, regardless of its location. This

includes off-site access to the school network from school or privately-owned/leased equipment.

2. FreshSteps user agreements will cover all employees, all students, and any other individuals authorised to make use of the school Internet facilities and ICT devices/equipment, such as teacher trainees, external tutors and providers, contractors, and other special visitors to the school.
3. Use of the Internet and the ICT devices/equipment by staff, students and other approved users at FreshSteps be limited to educational, professional development, and personal usage appropriate in the school environment, as defined in individual use agreements.
4. Signed use agreements will be filed in a secure place, and an appropriate system devised which facilitates confirmation that particular individuals are authorised to make use of the Internet and ICT devices/equipment.
5. The school has the right to monitor, access and review all use. This includes personal emails sent and received on the schools computer/s and/or network facilities at all times.
6. The school has the right to audit at anytime any material on equipment that is owned or leased by the school. The school may also request permission to audit privately owned ICT devices/equipment used on the school site or at any school related activity.
7. Issues relating to confidentiality, such as sighting student or staff information, reasons for collecting data and the secure storage of personal details and information (including images) will be subject to the provisions of the Privacy Act 1993.

The safety of children is of paramount concern. Any apparent breach of cyber safety will be taken seriously. The response to individual incidents will follow the procedures developed as part of the school's cyber safety practices. In serious incidents, advice will be sought from an appropriate source and/or a lawyer with specialist knowledge in this area. There will be special attention paid to the need for specific procedures regarding the gathering of evidence in potentially serious cases. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency.

Prohibitions

The use of the Internet computer network for illegal, inappropriate, unacceptable, or unethical purposes by students or employees is prohibited. The activities listed below are strictly prohibited by all users of the network. FreshSteps reserves the right to determine if any activity not appearing in the list below constitutes an acceptable or unacceptable use of the network. These prohibitions are in effect any time school district resources are accessed.

- Use of the network for non-work or non-school related communications.
- Use of the network to access obscene or pornographic material.
- Use of the network to transmit material likely to be offensive or objectionable to recipients.
- Use of the network to participate in inappropriate and /or objectionable discussions or news groups.
- Hate mail, harassment, discriminatory remarks and other antisocial communications on the network.
- Use of the network which results in any copyright violation.
- The illegal installation, distribution, reproduction, or use of copyrighted software on district computers.
- Use of the network to intentionally obtain or modify files, passwords, or data belonging to other users.
- Use of the network to misrepresent other users on the network.
- Use of school technology or the network for fraudulent copying, communications or modification of materials in violation of local, state, and federal law.
- Loading, downloading, or use of unauthorized games, programs, files or other electronic media.
- Malicious use of the network to develop programs that harass other users or infiltrate a computer system and/or damage the software components of a computer system.
- Destruction of district computer hardware or software.
- Use of the network to participate in Internet Relay chats (on-line real-time conversations).
- Use of the network to facilitate any illegal activity.
- Use of the network to communicate through e-mail for non-educational purposes or activities.
- Use of the network for commercial or for-profit purposes.

Use of the network for product advertisement or political lobbying

Consequences of Abuse

Any user of the network, whether student or employee, who violates the prohibitions listed in this policy, engages in any other act determined to be unacceptable use of the network by school authorities, or violates any other policy governing use of school resources and copyright law, will have their user privileges revoked and may face other disciplinary procedures according to existing and applicable school policies. In addition, illegal use of the network, intentional deletion or damage to files of data, destruction of hardware, copyright violations, or any other activity involving the violation of these rules will be reported to the appropriate legal authorities for prosecution.

Acceptable Use Policy Consent Form

Links with other policies

Safeguarding Policy

Behaviour policy