Glebe House

Friends Therapeutic Community Trust

IT Policy

September 2021

IT POLICY

Contents:

Statement of intent

At Glebe House, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for learners and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all learners and staff.

The school is committed to providing a safe learning and teaching environment for all learners and staff, and has implemented important controls to mitigate the risk of harm.

1. Legal framework

1.1. This policy has due regard to all relevant legislation including, but not limited to:
- The General Data Protection Regulation
- Freedom of Information Act 2000

1.2. This policy also has regard to the following statutory guidance:
- DfE (2021) 'Keeping children safe in education'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- This policy will be used in conjunction with the following school policies and procedures:
    - Acceptable Use Agreement
    - Safeguarding Policy
    - Behaviour Policy

2. Use of the internet

2.1. The school understands that using the internet is important when raising educational standards, promoting learner achievement and enhancing teaching and learning.

2.2. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all learners, though there are a number of controls the school is required to implement to minimise harmful risks.

2.3. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including the following:
- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. content involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

3.1. It is the responsibility of all staff to be alert to possible harm to learners or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.

3.2. The trustees are responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard learners.

3.3. The Head of School is responsible for ensuring the day-to-day e-safety in the school and managing any issues that may arise.

3.4. The Head of School will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach learners about online safety.

3.5. The Head of School and data protection officer (DPO) will ensure there is a system in place which monitors and supports the data protection requirements.

3.6. The Head of School will establish a procedure for reporting incidents and inappropriate internet use, either by learners or staff.

3.7. The Head of School will ensure that all members of staff are aware of the procedure when reporting e-safety incidents and will keep a log of all incidents recorded.
3.8. The SMT and Head of School will hold regular meetings with the Senior Manager responsible for IT and school network to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school's duty of care.
3.9. The Education Sub-committee will evaluate and review this E-safety Policy on an annual basis, considering the latest developments in ICT and the feedback from staff/learners.
3.10. The Head of School will review and amend this policy, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
3.11. Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.
3.12. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-safety Policy.
3.13. All staff and learners will ensure they understand and adhere to our Acceptable Use Agreement, which they must sign and return to the Head of School.
3.14. All learners are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

4. E-safety education Educating learners:

4.1. An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that learners are aware of the safe use of new technology both inside and outside of the school.
4.2. Learners will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material, and the validity of website content.
4.3. Learners will be taught to acknowledge ownership of information they access online, in order to avoid copyright infringement and/or plagiarism.
4.4. Clear guidance on the rules of internet use will be presented in all classrooms.
4.5. Learners are instructed to report any suspicious use of the internet.
4.6. PSHE lessons will be used to educate learners about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.
4.7. The school will hold e-safety events, such as Safer Internet Day and Anti-Bullying Week, to promote online safety.

Educating staff:

4.8. E-safety training opportunities is available to all staff members.
4.9. All staff will employ methods of good practice and act as role models for learners when using the internet and other digital devices.
4.10. All staff will be educated on which sites are deemed appropriate and inappropriate.
4.11. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
4.12. Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-safety Policy.

5. E-safety control measures Internet access:

5.1. Internet access will be authorised once learners have returned the signed Acceptable Use Agreement.
5.2. A record will be kept by the Head of School of all learners who have been granted internet access.
5.3. All learners will be provided with usernames and passwords and these will be held by the education staff. The education staff will log learners in when required in the course of a lesson or out of school activity.
5.4. All learners will be monitored continuously by a member of the education staff when they use computers that have internet access.
5.5. Learners' passwords will expire every month, and their activity is continuously monitored.
5.6. Effective filtering systems will be established to eradicate any potential risks to learners through access to, or trying to access, certain websites which are harmful or use inappropriate material.
5.7. Filtering systems will be used which are relevant to learners' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
5.8. The Trustees will ensure that the use of appropriate filters and monitoring systems does not lead to 'over blocking' – unreasonable restrictions as to what learners can be taught with regards to online teaching and safeguarding.
5.9. Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the Head of School.
5.10. The Senior network Manger will ensure all school systems will be protected by up-to-date virus software.
5.11. An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.

Email:

5.12. Learners will be given approved email accounts and are only able to use these accounts.
5.13. The use of personal email accounts by learners to send and receive personal data without permission is prohibited.
5.14. No sensitive personal data shall be sent to any other learners, staff or third parties via email.
5.15. Learners are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.
5.16. Any emails sent by learners to external organisations will be overseen by their class teacher and must be authorised before sending.
5.17. Chain letters, spam and all other emails from unknown sources will be deleted without opening.

Network security:

5.18. Network profiles for each learner and staff member are created in which the individual must enter a username and personal password when accessing the ICT systems within the school.
5.19. Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.
5.20. Passwords will require a mixture of letters, numbers and symbols to ensure they are secure as possible.
5.21. Passwords will expire after a month to ensure maximum security for learner and staff accounts.

Virus management:

5.22. Technical security features, such as virus software, are kept up-to-date and managed by the network manager.
5.23. The network manager will ensure that the filtering of websites and downloads is up-to-date and monitored.
5.24. Firewalls will be switched on at all times the network manager will review these on a weekly basis to ensure they are running correctly and to carry out any required updates.
5.25. Firewalls and other virus management systems, e.g. anti-virus software, will be maintained by the Network and IT Manager.
5.26. Staff members will report all malware and virus attacks to network manager.

6. Cyber bullying

6.1. For the purposes of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive messages, or the posting of information or images online.
6.2. The school recognises that both staff and learners may experience cyber bullying and is committed to responding appropriately to instances that should occur.
6.3. The school will regularly educate staff, learners and parents on the importance of staying safe online, as well as being considerate to what they post online.
6.4. Learners will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.
6.5. The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and learners.
6.6. The school has zero tolerance for cyber bullying, and any incidents will be treated with the utmost seriousness and will be dealt with in accordance with our safeguarding policy.

7. Reporting misuse

7.1. Glebe house School will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement, ensuring all learners and staff members are aware of what behaviour is expected of them.
7.2. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to learners as part of the curriculum in order to promote responsible internet use.

Misuse by learners:

7.3. Teachers have the power to discipline learners who engage in misbehaviour with regards to internet use.
7.4. Any instances of misuse should be immediately reported to the head of school through the Arbor system.
7.5. Any learner who does not adhere to the rules outlined in our Acceptable Use Agreement and is found to be wilfully misusing the internet will have a letter sent to the Registered Manager explaining the reason for suspending their internet use.
7.6. Complaints of a child protection nature, such as when a learner is found to be accessing extremist material, shall be dealt with in accordance with our Safeguarding Policy.

Misuse by staff:

7.7. Any misuse of the internet by a member of staff should be immediately reported to the Head of School and would normally be discussed in the SMT team. The SMT will deal with such incidents in accordance with the policies outlined in the staff handbook and may decide to take disciplinary action against the member of staff.

Use of illegal material:

7.8. In the event that illegal material is found on the school's network, or evidence suggests that illegal material has been accessed, the police will be contacted.

7.9. Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.

7.10. If a child protection incident is suspected, the school's child protection procedure will be followed – the DSL and Head of School will be informed and the police contacted.

7.11. Staff will not view or forward illegal images of a child. If they are made aware of such an image, they will contact the DSL.

8. Monitoring and review

8.1. The Head of School will evaluate and review this IT Policy on a yearly basis, taking into account the latest developments in ICT and feedback from staff/learners.

8.2. This policy will also be reviewed on an annual basis by the education subcommittee; any changes made to this policy will be communicated to all members of staff.

8.3. Members of staff are required to familiarise themselves with this policy as part of their induction programmes.

8.4. The date for the next review of this policy is September 2022.