2024 E-safety Policy

Last reviewed February 2024

1. Scope and Summary

1.1. E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

1.2. St Giles' e-safety policy operates in conjunction with St Giles' other policies, specifically but not limited to our safeguarding policy, our ICT policy, our PREVENT policy and our bullying and harassment policy.

2. Writing and reviewing the e-safety policy

2.1. Each UK School appoints an e-Safety Coordinator. This is automatically the school's Designated Safeguarding Lead, unless clearly stated in this policy.

2.2. Our e-Safety Policy has been written by the UK school Principals, building on the Cambridge e-safety policy (https://campartnership.org/wp-content/uploads/2022/01/CMAT-Esafety-Policy-2019.pdf) and government guidance. It has been agreed by St Giles' CEO and the UK school Principals.

2.3. The e-Safety Policy and its implementation will be reviewed annually.

2.4. The e-Safety Policy was revised on the date above by the Cambridge Principal.

3. Managing Internet access - why Internet use is important

3.1. The Internet is an essential element in 21st century life for education, business and social interaction. St Giles has a duty to provide students with secure Internet access as part of their learning experience.

3.2. Internet use is a part of St Giles' curriculum and a necessary tool for staff and students.

4. Safeguarding and security in the schools

4.1. Student access to the Internet will include appropriate filtering.

4.2. All staff and students will have clear rules for acceptable Internet use and procedures to follow to report unacceptable use (see appendix 1).

4.3. The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

4.4. Virus protection and security will be reviewed regularly and strategies will be discussed with ST Giles' ICT department.

5. St Giles' web site

5.1. St Giles will publish contact addresses, e-mails and telephone numbers on its website.

5.2. Staff or students' personal information will not be published.

5.3. Written permission from students, or the parents of under-18 students, will be obtained before photographs or video of students are used for publicity and published on the St Giles web site.

5.4. Where permission has been given, photographs and video that include pupils will be selected carefully.

6. Mobile phones

6.1. Mobile phones can be used during lessons or formal school time under the supervision of a member of staff.

6.2. Using of mobile phones for the sending of abusive or inappropriate messages is forbidden.

7. Social Media

7.1. Students' attention will be drawn to the precautions needed when using social media.

7.2. Under-18 students must inform the Designated Safeguarding Person if they do not wish their photo to appear on social media.

7.3. Staff must not use social media to have contact with students under the age of 18 and are strongly discouraged from using social media to have contact with students aged 18 and over.

7.4 This includes and is not limited to 'following' someone or requesting that they 'follow' you on Instagram / TikTok / X etc. 'Adding' someone on Messenger / Discord / WhatsApp.

7.5 The only exception to this rule is via the **Emergency Phone** number. Students are asked to add this number and U18 students in particular are encouraged to add the number. Only designated staff members have access to the Emergency Phone. Any students who have left MUST be deleted from the phone as soon as possible after their leaving date.

8. Monitoring and assessing risks

8.1. All staff must read the relevant parts of the staff handbook before using any school ICT resource.

8.2. St Giles will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. St Giles cannot accept liability for the material accessed, or any consequences of Internet access.

8.3. St Giles will liaise with outside organisations to establish a common approach to e-safety within its schools.

8.4. The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

9. Communicating this policy to students

9.1. E-safety rules will be posted in the computer room and will be available on the e-school.

9.2. Students will be informed that network and Internet use will be monitored.

10. Communicating this policy to Staff

10.1. All staff will be given the St Giles e-Safety Policy and its importance will be explained.

10.2. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

11. Rules

11.1. Students must immediately tell a teacher if they receive offensive messages of any kind.

11.2. Students must immediately tell a teacher if they are the victim of ‘cyber-bullying’ or know of any ‘cyber-bullying’ incidents in the school.

11.3. Students must not reveal personal details of themselves or others in online communication, or arrange to meet anyone over the Internet.

11.4. Students are advised never to give out personal details of any kind which may identify them or their location.

11.5. If staff or students discover an unsuitable website, it must be reported to the e-Safety Coordinator.

12. Handling e-safety complaints

12.1. Complaints of Internet misuse will be dealt with by the school Principal.

12.2. Any complaint about staff misuse must be referred to the school Principal.

13. Protecting personal data

13.1. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

14. PREVENT policy

14.1. St Giles will not tolerate the use of any of its ICT equipment for activities that contravene its Prevent Policy. These activities include, but are not limited to, accessing extremist websites or using the Internet to exchange or encourage extremist views.

14.2. Staff or students who have concerns that St Giles’ ICT equipment is being used in contravention of its PREVENT policy must report their concerns to the school Principal.

St Giles
CAMBRIDGE

St Giles E-safety policy

St Giles wants to keep you safe when you use technology while studying with us. We need your help to do this. Please follow these simple rules:

- Mobile phones can only be used during lessons if your teacher says so.
- Do not use a computer or your mobile phone to send abusive or inappropriate messages.
- Be careful when using the Internet and social media (Facebook, Instagram, etc):
- Tell a teacher if you receive offensive messages of any kind.
- Tell a teacher if you are the victim of 'cyber-bullying' or if you know of any 'cyber-bullying' incidents in the school.
- Do not reveal personal details of yourself or others in online communication, or arrange to meet anyone over the Internet.
- Never to give out your personal details of any kind which may identify you or your location.
- If you discover an unsuitable website report it to the Principal.
- No-one over the age of 18 should add anyone 17 or younger on social media.
- This includes and is not limited to 'following' someone or requesting that they 'follow' you on Instagram / TikTok / X etc. 'Adding' someone on Messenger / Discord / WhatsApp.
- The only exception to this rule is via the **Emergency Phone** number. Students are asked to add this number and U18 students in particular are encouraged to add the number. Only designated staff members have access to the Emergency Phone. Any students who have left will be deleted from the phone as soon as possible after their leaving date.
- Tell the Principal if you do not wish your photo to appear on social media.
- Network and Internet use will be monitored.
- Speak to the Principal or Welfare Officer about an e-safety concerns you have.

You can ask the Principal to see a copy of our e-safety policy. It is also available on the e-school.

Update July 2023