E-Safety Policy

St. George's School
28 Priory Road
Dunstable
LU5 4HR

01582 661471
www.stgeorgesdunstable.co.uk
info@stgeorgesdunstable.co.uk

E-Safety Policy
Version 3
23 January 2019

1. Introduction

1.1. The subject of Computing is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at St. George's we need to build in the safe and responsible use of digital technologies, in order to arm our young people with the skills to access life-long learning and employment. E-safety involves pupils, staff and parents making best use of technology, information, training and this policy to create and maintain a safe digital environment for St. George's School.

2. Roles and Responsibilities

Headteacher

2.1. The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the e-Safety Coordinator.

2.2. The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is used in conjunction with our IT agency.

2.3. The Headteacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The E-Safety Co-ordinator

2.4. The E-Safety Co-ordinator takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy/documents.

2.5. The E-Safety Co-ordinator ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

2.6. The E-Safety Co-ordinator provides advice for staff.

2.7. The E-Safety Co-ordinator liaises with school Computing

technical staff.

2.8. The E-Safety Co-ordinator receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

3. Teaching and Learning

3.1. The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

3.1.1. The school Internet access will be designed expressly for pupil use including appropriate content filtering.

3.1.2. Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.

3.1.3. Pupils are taught the SMART rules to help keep them safe online. This is regularly refreshed and revisited.

3.1.4. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

3.1.5. As part of the new Computing curriculum, all year groups have digital objectives that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and cyber bullying.

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

3.2. Through computing, we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a

multi-ethnic society. We also measure and assess the impact regularly through meetings our SEN co-ordinator and individual teachers to ensure all children have equal access to succeeding in this subject. Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.

4. Social Networking

4.1. Social networking Internet sites (such as Twitter, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

4.2. Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.

4.3. Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos. This is also focused on as part our SMART rules topic.

4.4. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils as the legal age is 13 years old to hold an account.

4.5. Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.

4.6. Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites.

5. Reporting

5.1. All breaches of the e-safety policy need to be recorded in the E-Safety reporting book that is kept in the school office. The details of the user, date and incident should be reported. Incidents which may lead to child protection issues need to be passed on to one of the Designated Safeguarding Officer

immediately – it is their responsibility to decide on appropriate action not the class teachers.

5.2. Incidents which are not child protection issues but may require LT intervention (e.g. cyberbullying) should be reported to LT in the same day.

5.3. Allegations involving staff should be reported to the Headteachers. Evidence of incidents must be preserved and retained.

5.4. The curriculum will cover how pupils should report incidents (e.g. Trusted adult, Childline)

6. Mobile Phones

6.1. 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.

6.2. Pupils by permission of the Headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the school and collected at the end of the day.

6.3. Staff should always use the school phone to contact parents.

6.4. Staff including students and visitors are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers should ensure that their phones are stored safely away during the teaching day.

6.5. Staff may use their mobile phones in the staffroom/one of the school offices.

6.6. On trips staff mobiles are used for emergency only.

7. Digital/Video Cameras/Photographs

7.1. Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

7.2. Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.

7.3. Publishing of images, video and sound will follow the school policy.

7.4. Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

7.5. The Headteacher or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner

7.6. Staff should always use a school camera to capture images and should not use their personal devices. Photos taken by the school are subject to the Data Protection act.

8. Published Content and the School Website

8.1. The school website is a valuable source of information for parents and potential parents.

8.2. Contact details on the Website will be the school address, e-mail and telephone number.

8.3. Staff and pupils' personal information will not be published.

8.4. The Headteacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

8.5. Photographs and videos that include pupils will be selected carefully in line with our permissions.

8.6. Pupils' full names will not be used in association with photographs.

8.7. Consent from parents will be obtained before photographs of pupils are published on the school Website.

8.8. Work will only be published with the permission of the pupil.

8.9. Parents should only upload pictures of their own child/children onto social networking sites.

9. Protecting Personal Data

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

10. Assessing Risk

10.1. The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit Computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

11. Handling E-Safety Complaints

11.1. Complaints of Internet misuse will be dealt with by a senior member of staff.

11.2. Any complaint about staff misuse must be referred to the Headteacher.

11.3. Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.

11.4. Pupils and parents will be informed of the complaints procedure.

11.5. Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

12. Communication of Policy

Pupils

12.1. Rules for Internet access will be posted in all networked rooms.

12.2. Pupils will be informed that Internet use will be monitored.

12.3. Pupils will be informed of the importance of being safe on social networking sites such as msn. This will be strongly reinforced across all year groups during ICT lessons and all year groups look at different areas of safety through the digital literacy lessons.

Staff

12.4. All staff will be given the School e-safety Policy and its importance explained.

Parents

12.5. Parents' attention will be drawn to the School e-safety Policy in newsletters and on the school Website.

Useful resources:

- https://www.childnet.com/
- https://www.saferinternet.org.uk/
- https://www.net-aware.org.uk/

23 January 2019

Stuart Compton, Acting Head Teacher