2019

Online Safety Policy

Implemented: September 2019

To be reviewed: September 2020

Review frequency: Annually

Consultation process

SLT, computing leader, safeguarding governor

Signed (HT)

(COG)

"In everything we do today, we're following Jesus and his way."

Online safety policy

Context

Harnessing Technology: Transforming learning and children's services sets out the government plans for taking a strategic approach to the future development of Computing.

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

The Online Harms White Paper sets out the government's plans for a world-leading package of online safety measures that also supports innovation and a thriving digital economy. This package comprises legislative and non-legislative measures and will make companies more responsible for their users' safety online, especially children and other vulnerable groups.

The Online Harms White Paper aims to allow:

- A free, open and secure internet.
- Freedom of expression online.
- An online environment where companies take effective steps to keep their users safe, and where criminal, terrorist and hostile foreign state activity is not left to contaminate the online space.
- Rules and norms for the internet that discourage harmful behaviour.
- The UK as a thriving digital economy, with a prosperous ecosystem of companies developing innovation in online safety.
- Citizens who understand the risks of online activity, challenge unacceptable behaviours and know how to access help if they experience harm online, with children receiving extra protection.
- A global coalition of countries all taking coordinated steps to keep their citizens safe online.
- Renewed public confidence and trust in online companies and services.

The Green Paper *Every Child Matters* and the provisions of the *Children Act 2004*, *Working Together to Safeguard Children* sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The ‘staying safe’ outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Much of these aims apply equally to the ‘virtual world’ that children and young people will encounter whenever they use technology in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that modern technology can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the ‘virtual’ or digital world as would be applied to the school’s physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

1. The technologies

Computing in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (apps and web clients) (WhatsApp, Facebook messenger, Chatroulette, Snapchat, Houseparty, FaceTime, PlayStation/Xbox console messenger. etc.) often using simple web cams / built in phone cameras.
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular: Facebook, Twitter, Instagram, Snapchat, Pinterest, Reddit, Myspace, Tumblr, Skype, WeChat.)
- Video broadcasting sites (Popular: YouTube, Twitch, Periscope)
- Chat Rooms (Popular: Teenchat, Habbo Hotel, Houseparty, Discord.
- Gaming Sites (Popular: Neopets, Miniclip, Runescape, Twitch)
- Music download sites (Popular itunes, Spotify, Napster, Deezer)
- Mobile phones with camera and video functionality (FaceTime, Skype)
- Smart phones with e-mail, web functionality and cut down 'Office' applications.
- Games machine consoles – PlayStation, Xbox, Wii, DS etc.

2. Managing the Internet Safely

The following principles will be implemented to ensure safe access and use of the Internet:

- All Internet activity should be appropriate to staff professional activities or the children's education;

- Internet access is limited using the LGfL filter, which prevents access to many inappropriate or unknown sites;

- Children's access to the internet will only be allowed under adult supervision.

- Access is limited to the use of authorised accounts and passwords, which should not be made available to any other person;

- Activity that threatens the integrity of the school's computer systems, or that attacks or corrupts other systems, is prohibited;

- Copyright of materials must be respected;

3. Managing Email Safely

The following principles will be implemented to ensure safe use of email facilities:

- Pupils may only use approved e-mail accounts on the school system (E.g. DB Primary and LGFLmail).

- Pupils are taught to immediately tell a teacher if they receive offensive e-mail.

- Pupils are taught to not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

- The forwarding of chain letters is not permitted.

4. Publishing Safely

The school wishes the school's web site to reflect the diversity of activities, individuals and education that can be found at St. George's. However, the school recognises the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the Internet, the following principles should be borne in mind:

- No video recording or photo may be made or published without the written consent of the parents/legal guardian of the child concerned, and the child's own verbal consent.

- Surnames of children should not be published, especially in conjunction with photographic or video material.

- No link should be made between an individual and any home address (including simply street names).

- No material may be published on the school web site without approval of the Computing co-ordinator.

5. Roles and Responsibilities

e-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the Policy is implemented and compliance with the Policy monitored.

Our school **Online Safety lead** is Mr Antony Gavas.

Our Online Safety leader ensures they keep up to date with Online Safety issues and guidance through use of organisations such as LGFL and The Child Exploitation and Online Protection (CEOP). The school's e-Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of Online Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on Online Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school Online Safety procedures. Central to this is fostering a ‘No Blame’ culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools’ Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- eBullying / Cyberbullying procedures;
- their role in providing e-Safety education for pupils;

Staff are reminded / updated about Online Safety matters at least once a year.

In addition, staff must ensure that mobile phones and personally-owned devices are not used in any way during lessons or formal school time. They should be on silent and kept in a bag/cupboard at all times whilst in the presence of children. Mobile phones must not be used in the school corridors.

6. Pupils

The school implements an online safety scheme of work which has been agreed by staff. Children take part in online safety lessons and activities during internet safety day in February and at other times linked to Computing lessons, PSHE and other areas of the curriculum.

The school has an Acceptable Use Agreement. Pupils in KS2 sign the agreement; KS1 children sign a simplified version; Foundation pupils are made aware of the policy. Parents/Guardians sign the Agreement to confirm that they have discussed the Agreement with their child. Pupils have to click to agree to these rules before every log on.

7. Parents

Parents are updated about online safety issues at least annually. This can take the form of meetings, newsletters, links to information etc.