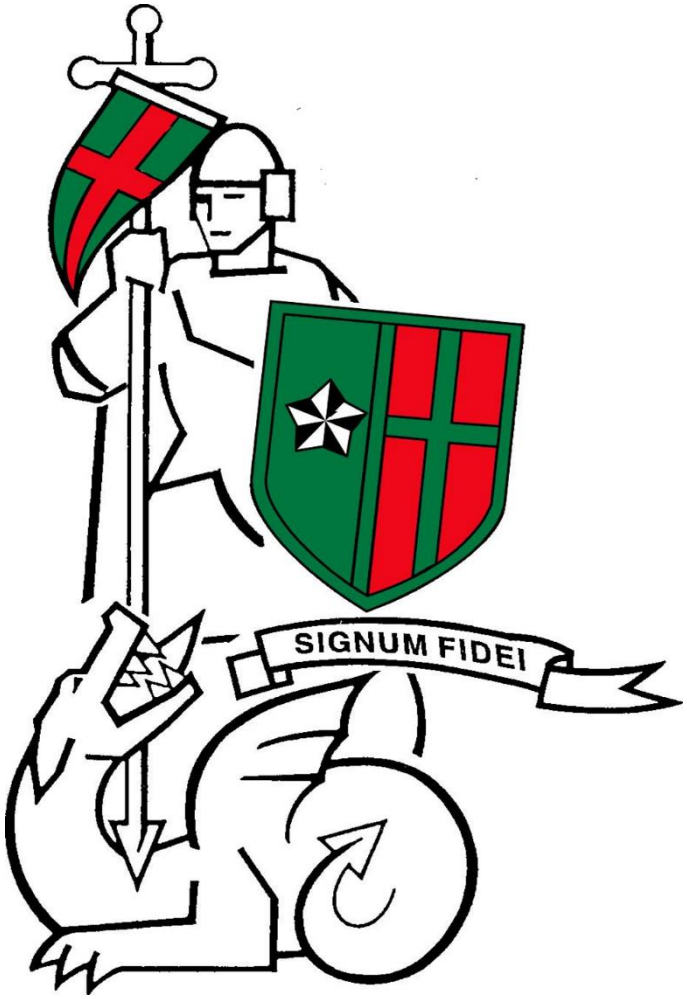

St George's RC Primary School
Internet Access Policy
June 2017

Contents:

Statement of intent

Statement of intent

At St George's RC School, 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 pupils 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 pupils and staff.

The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

Signed by:

_____	Headteacher	Date: _____
_____	Chair of governors	Date: _____

1. Legal framework

1.1. This policy has due regard to the following legislation, including, but not limited to:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997

1.2. This policy also has regard to the following statutory guidance:

- DfE (2016) 'Keeping children safe in education'

1.3. This policy will be used in conjunction with the following school policies and procedures:

- E-security Policy
- Digital Safeguarding Policy
- Cyber Bullying Policy
- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement

2. Use of the internet

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

2.2. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, 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:

- 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. 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 pupils 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 governing body is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.

3.3. The e-safety officer, Mr Ryan de Koning working with Ms Kat Chandler, is responsible for ensuring the day-to-day e-safety in the school, and managing any issues that may arise.

3.4. The e-safety officer is responsible for chairing the e-safety committee, which includes representatives of the school senior leadership team (SLT), teaching staff, governors, parents, pupils and wider school community.

3.5. The headteacher is responsible for ensuring that the e-safety officer and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.

3.6. The e-safety officer 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 pupils about online safety.

3.7. The headteacher will ensure there is a system in place which monitors and supports the e-safety officer, whose role is to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.

3.8. The e-safety officer will regularly monitor the provision of e-safety in the school and will provide feedback to the headteacher.

3.9. The e-safety officer will maintain a log of submitted e-safety reports and incidents.

3.10. The headteacher will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.

3.11. The e-safety officer 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.

3.12. Cyber bullying incidents will be reported in accordance with the school's Anti-Bullying and Harassment Policy.

3.13. The Headteacher will hold regular meetings with the e-safety officer 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.

3.14. The governing body will evaluate and review this E-Safety Policy on a regular basis, taking into account the latest developments in ICT and the feedback from staff/pupils.

3.15. Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.16. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-Safety Policy.

3.17. All staff and pupils will ensure they understand and adhere to our Acceptable Use Agreement.

3.18. Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

3.19. The headteacher is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

3.20. All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

4. E-safety education

4.1. Educating pupils:

- An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.
- Pupils 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.
- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in all classrooms.
- Pupils are instructed to report any suspicious use of the internet and digital devices.
- PSHE lessons will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.
- The school will hold e-safety events, such as Safer Internet Day and Anti Bullying Week, to promote online safety.

4.2. Educating staff:

- A planned calendar programme of e-safety training opportunities is available to all staff members, including whole school activities and CPD training courses.
- All staff will undergo regular audits by the e-safety officer in order to identify areas of training need.
- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- The e-safety officer will act as the first point of contact for staff requiring e-safety advice.

4.3. Educating parents:

- E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media.
- Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any e-safety related concerns.

5. E-safety control measures

5.1. Internet access:

- Internet access will be authorised once parents and pupils have returned the signed consent form in line with our Acceptable Use Agreement.
- A record will be kept by the class teacher of all pupils who have been granted internet access.
- All users will be provided with usernames and passwords, and are advised to keep these confidential to avoid any other pupils using their login details.
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access,

certain websites, which are harmful, or use inappropriate material.

- Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the headteacher.
- All school systems will be protected by up-to-date virus software.

  Inappropriate internet access by staff may result in appropriate disciplinary action as per Staff Code of Conduct.

5.2. Social networking for staff

- Staff sign and understand the staff code of conduct which explains about appropriate social media usage.

5.3. Published content on the school website and images:

- The headteacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Staff are able to take pictures, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take pictures using their personal equipment.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

5.4. Mobile devices and hand-held computers:

- The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.
- Children will hand their mobile devices into the school office every morning and collect them at home time.

6. Cyber bullying

6.1. The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

7. Reporting misuse

7.1. St George's RC School will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement, ensuring all pupils 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 pupils as part of the curriculum in order to promote responsible internet use.

7.3. **Misuse by pupils**

7.4. Any misuse by pupils will be reported to the class teacher, then Headteacher and CYC if appropriate. Eg: in the case of a stricter filter system being implemented.

7.5. **Use of illegal material:**

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

- If a child protection incident is suspected, the school's child protection procedure will be followed – the DSL and headteacher will be informed and the police contacted.

8. Monitoring and review

8.1. The e-safety committee will evaluate and review this E-Safety Policy on a regular basis, taking into account the school's e-safety calendar, the latest developments in ICT and the feedback from staff/pupils.

8.2. This policy will also be reviewed on a regular basis by the governing body; any changes made to this policy will be communicated to all members of staff.