ST GEORGE'S CHURCH OF ENGLAND FOUNDATION SCHOOL

"Every moment, every day, every individual counts"

ONLINE SAFETY AND ACCEPTABLE USE POLICY

Last Reviewed: ***November 2019***

Date for Review: ***November 2020***

Governors Monitoring Pair:	Safeguarding
SLT Responsible:	Deputy Headteacher
Review Period:	Annually

St George's C of E Foundation School

Online Safety and Acceptable Use Policy

The School's Online Safety Policy replaces the Internet Policy to reflect the need to raise awareness of the Online Safety issues associated with information systems and electronic communications as a whole.

Safeguarding and therefore, online safety is identified as a responsibility for ALL members of staff in school.

1. Online Safety Education:

This is a safeguarding concern and all pupils will receive a minimum of 5 lessons per academic year on the updated Online Safety Rules and Policies within the School. This is carried out in the ICT curriculum for Years R – 10. Year 11 have an Online Safety Worship time and Years 12 and 13 have Online Safety awareness in their worship time and through Citizenship days. The school also takes part in the annual Safer Internet morning.

2. Staff and Pupil Electronic Communications:

Staff and pupils need to understand that the School's network is a privilege and can be removed should it be necessary. The School monitors all network and internet use to ensure pupils safety. All users are expected to adhere to the generally accepted rules of (netiquette) including all of the following:

- People you don't know are strangers
- Tell an adult if you get that 'uh oh' feeling
- Be polite.
- Use of appropriate language.
- Do not use abusive language in your messages to others.
- Do not reveal the addresses, phone numbers or personal addresses of yourself or others.
- No pupil mobile numbers should be held on any telephones by staff.
- Illegal activities are strictly forbidden.
- Email is not guaranteed to be private.
- System administrators monitor and have access to all emails.
- Messages relating to illegal activities will be reported to the authorities.

3. Using New Technologies in Education:

All new technologies should be looked at for their educational benefit and a risk assessment carried out before use in school is allowed.

- No mobile phones are to be used by pupils for any purpose whilst on the school premises.
- Mobile telephones with the power of a pc may come with internet, Bluetooth and infrared (IR) and a camera.
- New learning environments such as Sharepoint.
- Internet voice and messaging such as Skype and Interactive Whiteboard (IWB) Linking.
- Digital story telling involving independence of thought and self motivation.
- Podcasting, broadcasting and recording lessons.
- Digital video.
- Online safety is taught across the whole curriculum.

- All members of staff have a responsibility to provide a safe environment in which all pupils can learn, this includes the online environment in which pupils now live and learn and it is the responsibility of all staff to reference ways in which safeguarding and online safety can be developed and embedded.

Responding to Concerns:
All staff at St George's Church of England Foundation School are aware that abuse, neglect and safeguarding issues are rarely standalone. Online safety is a key issue to ensure we safeguard all our pupils.

At St George's Church of England Foundation School it is our responsibility to specifically identify that online or Cyberbullying can result in emotional abuse. This is also addressed in the Anti-Bullying Policy, where we will respond to any concerns reported.

Regarding sexual abuse this can occur via the internet and can involve a range of activities, including, but not limited to online grooming and exploitation, exposure to pornographic content and engaging a child in sexual activity online. This also identifies that perpetrators can be male or female and may include children themselves (e.g. sexting, also known as YPSI). It is the responsibility of St George's Church of England Foundation School to ensure that all our pupils are safeguarded against online sexual abuse.

Sexting is an increasingly common activity among children and young people where they share inappropriate or explicit images online. This sharing of images is via mobile phones, webcams, social media and instant messaging.

This sharing of images is totally inappropriate, distribution of images can lead to prosecution and it can lead also to blackmail, bullying and emotional distress.

All members of staff at St George's Church of England Foundation School know how to respond appropriately to sexting concerns and have received training around this. They are also made aware of the potential risks pupils face when using technology, and the implications of the risks to pupils who send inappropriate images.

Staff are told that should they feel they are being subjected to online abuse they must report this.

All staff and pupils at St George's Church of England Foundation School are aware of the dangers of Child Sexual Exploitation (CSE) and radicalisation, both of which can occur online. Tools are used by the school to monitor this and concerns are reported immediately to the appropriate authorities.

All staff and Governors have been sent Powerpoints on the signs of CSE, how to spot them and how to respond to them. These are available on the staff shared area and are updated by the Designated Safeguard Lead.

Staff, Governors and pupils are aware of the risks of radicalisation and grooming online. The Prevent Team have been into school and educated staff and Governors on the Prevent Duty and Radicalisation. The educate against hate link can be found on the school website. APP has been sent to all staff and Governors highlighting the changes of online grooming. It is also available on the staff shared area and is updated by the Designated Safeguard Lead.

All pupils, staff and Governors are continually reminded about the potential risks online that can be encountered.

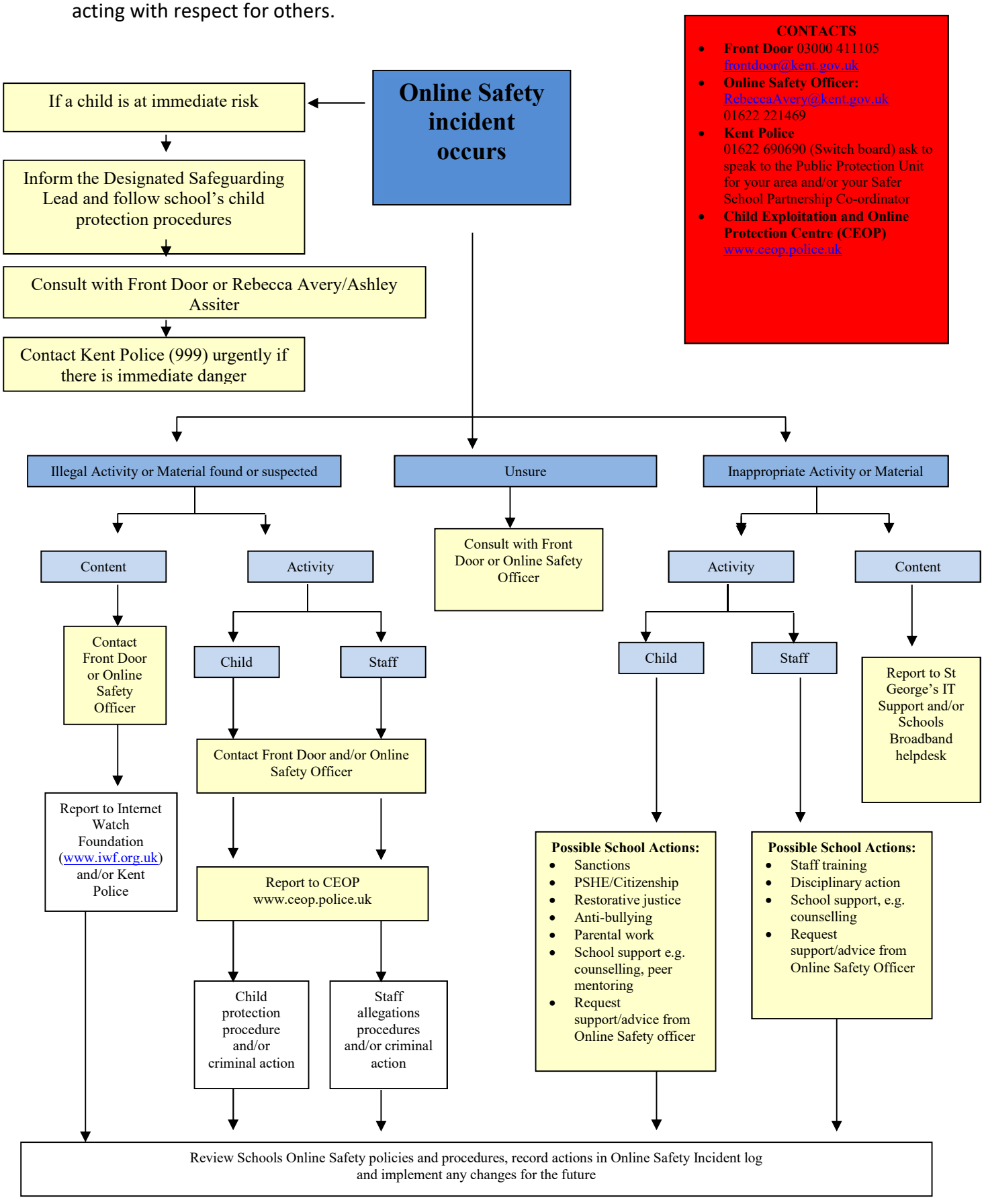
All appropriate filters are in place as recommended by UK Safe Internet Centre, appropriate filtering also monitored.

All pupils and staff sign the Acceptable Use Policy to ensure appropriate use of technology. Any breach of this is dealt with by contacting parents and re-educating pupils.

Up to date training for all staff is regulated by the local E-Safety Co-ordinator (Ashley Assiter/Rebecca Avery

4. Response to an Incident of Concern:

An Online Safety policy should recognise and seek to develop the skills that young people need when communicating and using these technologies properly while keeping safe and secure and acting with respect for others.



5. Electronic Communication Includes:

- Internet collaboration tools i.e. Social networking sites such as Twitter, Facebook and blogs.
- Internet research such as web browsers, search engines.
- Mobile phones and personal digital assistance (PDA).
- Internet communications email and Instant Messaging.
- Webcams.
- Wireless games consoles.

Risks Involved with the use of these are:

- Receiving inappropriate content.
- Predation and grooming
- Requests for personal information
- Viewing incitement sites
- Bullying and threats
- Identity theft publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information
- Hacking and security breaches
- Corruption or misuse of data

6. School Responsibilities:

Online Safety is a relatively new concept and covers a wider scope than internet use, hence the need for schools Online Safety responsibilities.

- The School has appointed an Online Safety coordinator who is Judy Wreford (Deputy Headteacher), who is the Designated Safeguarding Lead. The Online Safety coordinator can receive support and advice from the Children, Families and Education Online Safety Officer, Children's Safeguard Service and as and when necessary the Police.
- The Online Safety Coordinator is responsible for maintaining the Online Safety Policy
- Managing the Online Safety Training and keeping updated on local and national Online Safety awareness campaigns
- The school reviews its policy annually to ensure it is current and considering any emerging technologies.
- The School audits its filtering system regularly in order to ensure that inappropriate websites are blocked.
- Any incidents of possible misuse by staff or pupils are fully investigated and appropriate action is taken
- The School's Online Safety is included in the curriculum and ensures that every pupil has been educated about safe and responsible use.
- All staff must read and sign the School's Code of Practice
- Parents and pupils must sign the Online Safety Rules and Consent Form
- The School's Online Safety Policy is available to all staff, pupils, parents and visitors.
- Online safety co-ordinator is responsible for ensuring that all members of staff access appropriate safeguarding training, including online safety.

7. Implementation and Compliance:

It is essential that staff remain vigilant in planning and supervising appropriate educational and ICT experiences. No policy can protect pupils without this effective implementation.

- Pupils are constantly reminded of their responsibilities with the display of posters in all rooms, with or without computers.
- All staff, pupils and parents are aware of how to report an incident of concern regarding internet misuse.
- Filtering is managed by the Local Authority, System Providers and internally and this is approved and managed by a member of the Senior Leadership Team and the Online Safety Coordinator. A report can be provided by the School's IT Support Team of overall use of computers and any misuses by staff/pupils is given to the Online Safety Co-ordinator.

8. The writing and review of Online Safety Policy:

- The School's Online Safety Policy has been written by the school built on the KCC Online Safety Policy and Government Guidelines.
- The Policy has been agreed by the Senior Leadership Team and approved by the Governing Board.
- The Online Safety Policy and its implementation is reviewed **annually**.
- Training for DSL is updated at least within every two years.
- Staff training takes place every year where possible.
- Outside professionals are invited in to train staff on specific online concerns.

9. Why is the Internet Use Important?

The rapid development of electronic communications are having a profound effect on society hence the reason it is necessary and important to enable our pupils to achieve education through ICT and Internet use.

- The purpose of Internet use in St. George's C of E Foundation School is to raise educational standards, promote individual achievement and to support the professional work of staff in order to enhance the learning ability of pupils.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- All pupils who show a responsible and mature approach have an entitlement to internet access.
- The use of the internet is an essential part of the 21st century for life, education, and business and social interaction. Therefore, it is the duty of the school to provide pupils with a quality internet access as part of their learning experience.
- Use of the internet outside of school is exhaustive and pupils need to learn how to evaluate internet information and to take care of their own safety and security whilst online.

10. How does internet use benefit education?

Access to worldwide educational resources including museums and art galleries

- Inclusion in the Nation Education Network which connects all UK Schools.
- Educational culture exchanges between pupils worldwide
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across support services and professional associations.
- Exchange of administration and curriculum with KCC and DFE.

11. How Can Internet Use Enhance Learning?:

- St. George's C of E Foundation School Internet access is expressly designed for pupil use and is filtered appropriate to the age of pupils.
- Pupils are taught what internet use is acceptable and what is not and pupils are given clear guidelines for internet use.
- Internet access is planned to enrich and extend learning activities.
- Access levels are reviewed annually to reflect the curriculum requirement and age of pupils.
- Staff guide pupils in online activities that support the learning outcomes planned for the pupil's age and maturity.
- Pupils are educated in the effective use of the internet for research including the skills of knowledge, location, retrieval and evaluation.

12. How Pupils Learn To Evaluate Internet Content:

- St. George's C of E Foundation School ensures that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy.
- Pupils are taught how to acknowledge and resource information gained.

13. How Is Information Systems Security Maintained?

- Users are taught to take responsibility for their network use.
- All work stations are locked when left unsupervised.
- All servers are located securely and access is restricted to network technicians.
- The server operating system is secured and kept up to date.
- Virus protection for the whole school network and is installed and automatically updated by the provider (Capita). IT Support follow the guidance of the Kent Online Safety Policy.
- Access by wireless is proactively managed.
- Guest wireless is managed by a secure key id.

Local Area Network (LAN) security issues include:

- Servers are located securely and physical access is restricted.
- The server operating system is secured and kept up to date.
- Virus protection for the whole system is installed and current.
- Wireless by devices is pro-actively managed.

14. Wide Area Network (WAN) security issues include:

- All internet connections are arranged by the Kent Community Network (KCN) to ensure compliance with the security policy.
- KCN firewalls and switches are configured to prevent unauthorised access between schools.
- Decisions on Wider Area Network security are made on a partnership between St. George's C of E Foundation School and KCN.
- The security of St. George's C of E Foundation School information system is regularly monitored and reviewed.
- Virus protection is updated regularly.
- Security strategies are discussed with Education Information Support (EIS)/ Capita.
- Pupil data sent over the internet is encrypted and secure.
- Unapproved system utilities and executable files are not allowed in pupils' work areas or attached to emails.

- Files held on the School's network are regularly checked and the capacity of the networks is regularly monitored.
- Portable media may not be used without specific permission followed by a virus check.

How Cyberbullying is managed:

- Cyberbullying (along with all forms of bullying) is not tolerated at St George's C of E Foundation School.
- There are clear procedures in place to support anyone affected by Cyberbullying.
- All incidents reported to school are recorded.
- Pupils, staff and parents are advised to keep a record of the bullying as evidence.
- St George's C of E Foundation School takes steps to identify the bully and where appropriate interview any possible witness, and if necessary contact the police.
- Any pupil caught Cyberbullying may have their internet access suspended for a period of time.
- Where appropriate the police are contacted if a criminal offence is suspected.

How Learning Platforms (LP) and Learning Environments are managed:

- The Senior Leadership Team and staff are responsible for monitoring the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff are advised on acceptable conduct and use when using the LP.
- When staff or pupils leave the school their accounts are disabled.
- Any concerns regarding inappropriate use of the LP are referred immediately to the Online Safety Co-ordinator.

15. How is email managed? (Secondary only):

Email is an essential part of communications for staff and Secondary pupils. The implications for email use for school community is thought through thoroughly and appropriate Online Safety measures put in place.

- Pupils at St. George's C of E Foundation School may only use approved email accounts.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in communication or arrange to meet anyone without specific permission.
- Pupils should not access external personal email accounts on school computers in school.
- Staff will only use official school provided email accounts to communicate with pupils and parents, as approved by the Senior Leadership Team.

16. How Published Content is Managed?

- Contact details on the website are the school address, email and telephone number.
- Staff and pupil personal information is not published.
- The Headteacher takes overall editorial responsibility and ensures that content is accurate and appropriate in liaison with the Examinations Officer.
- St. George's C of E Foundation School Website complies with the School's guidelines for publications including respect for intellectual property rights and copyright.

17. Publishing of Pupil Images and Work:

The security of staff and pupils at St. George's C of E Foundation School is of paramount importance. The publishing of pupil full names and their images is not acceptable.

- Pupils full names are not used anywhere on the website, particularly in association with photographs.
- Written permission from parents is obtained when their child joins the school, with the option for their child to be included in a No Publicity list.
- The School has a Policy regarding the use of photographic images of children which outlines Policies and procedures (Image Use Policy).

18. Managing of Social Networking and Personal Publishing:

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content, examples includes Blogs, Twitter, Instagram, Facebook, chat rooms and several others.

- St George's C of E Foundation School blocks access to social networking sites.
- News groups are also blocked.
- Pupils are advised never to give out personal details of any kind which may identify them and/or their location, examples of this are their real name, address, mobile or landline phone numbers or school attended, IM (Instant Messenger) and e-mail addresses, full names of friends, specific interests in clubs etc.
- Pupils are advised not to place personal photos on any social network space, they should also consider how public the information is and advised to use private areas.
- Staff are also blocked from accessing social networking sites in school.
- All pupils have set passwords and are advised not to allow other individuals to use their passwords.
- Pupils are advised to only invite known friends and deny access to others.
- Pupils are aware that bullying can take place through social networking sites, especially when the space has been set up without a password and others are invited to see the bully comments.
- Staff, are continually reminded that they should not be running social network spaces for pupil use on a personal basis, also that they should not advertise on social media where they work
- Pupils are advised not to publish specific and detailed thoughts, especially those that may be considered threatening, hurtful and defamatory.

19. Managing Filtering:

Internet access is appropriate to all members of the school community. The technical strategies being developed to restrict access to inappropriate material fall into several overlapping types (known as filtering).

- St George's C of E Foundation School has filtering strategies in order to prevent access to unsuitable sites. This is continually maintained by the Broadband Provider (EIS) in order to monitor new sites that appear on a daily basis.
- Due to the blocking and filtering systems in place in St George's C of E Foundation School pupils inevitably have limited access to a range of information.
- Search engines are in place to safe search and filter outgoing information.
- There is a system in place in order that web browsers are set to reject unacceptable content.
- All access is monitored by staff and attempted access to forbidden sites is reported weekly to the online safety co-ordinator.
- St George's C of E Foundation School works with KCC, and the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved.
- Any staff or pupil discovering unsuitable sites are required to report the URL (Uniform Resource Locator) to the St George's IT Support Team, class teacher/any adult.

- The Online Safety Co-ordinator, who is a member of the Senior Leadership Team, regularly checks to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material considered by the school to be illegal is reported to appropriate agencies for example IWF (Internet Watch Foundation) or CEOP (Child Protection and Online Protection Centre).
- The schools filtering strategy is designed by educators to suit the age and curriculum requirements of all pupils.

20. The Management of Emerging Technologies:

Many emerging communication technologies offer the potential to develop new learning tools including mobile communications, wide internet access and multi-media.

- At St George's C of E Foundation School all emerging technologies are examined for educational benefit and a risk assessment is carried out before use in school is allowed.
- Mobile phones are not used whilst the pupils are on the school premises.
- The sending of abusive or inappropriate text messages is forbidden.

School phones are available for staff to use when contacting pupils or parents

21. Protecting Personal Data:

The quantity and variety of data held on pupils, families and staff is expanding quickly. While this data can be very useful in providing services, data could be mishandled, stolen or misused. The Data Collection Act 1998 and the Data Protection Act (2018) gives pupils the right to know what information is known about them and it provides a framework to ensure that personal information is handled properly. The Act applies to everyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information related to individuals. ***No pupil data to be held on C or Local Drives OF ANY SCHOOL COMPUTER, including laptops which may be taken off premises***. The Act sets 8 data protection principles which must be adhered to when processing personal data.

- Personal data at St George's C of E Foundation School is recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Any breaches in GDPR are reported immediately to the School DPO.

The 8 principles are that personal data must be:

- processed fairly and lawfully
- processed for specific purposes
- Adequate relevant and not excessive
- Accurate and up to date
- Held no longer than is necessary
- Processed in line with individual rights
- Kept secure
- Transferred only to other countries with suitable security measures

22. The Authorisation of Internet Access:

The school allows internet access to staff and pupils on the basis of educational need. Authorisation is on an individual basis. Parents permission is required in all cases.

- St George's C of E Foundation School maintains a current record of all staff and pupils who are granted access to the schools electronic communications via the St George's IT Support Team.
- All staff read and sign the staff information systems Code of Conduct before using any school ICT resource.
- St George's C of E Foundation School pupils have to individually agree to comply with the online safety rules before internet access is granted.
- Parents are required to sign and return a consent form for pupil access.
- Parents are informed that pupils are provided with supervised internet access.

23. The Assessment of the Risks:

As a result of the quantity and breadth of information available through the internet, and as this continues to grow, it is not possible to guard against every possible situation. As a result of this the school has a disclaimer as shown below:

St George's C of E Foundation School will take all reasonable precautions to ensure users access only appropriate material, however due to the global and connected nature of internet content it is not possible to guarantee that access to unsuitable material will never occur over a school computer. Neither the school or KCC can accept liability for the material accessed or any consequences resulting from internet use. The use of computer systems without permission or for inappropriate purposes can constitute a criminal offence over the Computer Misuse Act 1980

- Methods to assess and minimise risk are monitored regularly
- The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the School nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The School will audit ICT use to establish if the online safety Policy is adequate and that the implementation of the online safety policy is appropriate.

24. How Online Safety Complaints are Handled:

Parents, staff and pupils know how to submit a complaint. Prompt action is taken if a complaint is made.

- Complaints of internet misuse at St George's C of E Foundation School are dealt with by senior members of staff, the relevant Head of Year, Lead Learner or Director of Learning and/or relevant members of the Senior Leadership Team
- Any complaint about staff misuse is referred to the Headteacher
- Pupils and parents are informed of the complaints procedure
- Parents and pupil work together in partnership with staff to resolve issues
- Discussions are held with the local Police, Youth Crime Reduction Officer, PCSO to establish procedures for handling potentially illegal issues
- Sanctions within the school discipline policy include: interview by Online Safety Co-ordinator and re-signing of code of conduct, informing parents and removal of internet or computer access for a period of time
- Any child protection issue is referred immediately to the Designated Safeguarding Lead.

25. The Use of Internet Across the Community:

Internet access is available in many situations in the local community. In addition to the home, access may be available at the local library, youth club, adult education centre, village hall, or cyber-

café. It is expected that young people would encounter a consistent policy to the Internet use wherever they are.

- St George's C of E Foundation School liaises with off site institutions to establish a common approach to Online safety.
- The school is sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

26. How the Policy is Introduced to Pupils:

The majority of the pupils are very familiar with mobile and internet use and culture and therefore the pupil voice are involved in the designing of parts of the school's Online safety policy. The teaching of Online Safety is primarily an ICT responsibility; however this is also re-enforced across all other areas of the curriculum.

- Online safety posters are displayed in all rooms with and without internet access.
- Pupils are aware that network and internet use is constantly monitored.
- An Online safety training programme has taken place to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use takes place before internet access is granted.
- An Online safety module is included in the ICT programmes covering both school and home use.

27. How the Policy is discussed with Staff:

It is extremely important that all staff at St George's C of E Foundation School feel confident to use the new technologies in teaching. All staff are expected to subscribe to the values and methods of the school's Online safety policy. Staff are aware and understand the rules for information systems misuse for KCC employees.

- All staff are given the School Online safety and Acceptable Use Policy and its application and importance is explained.
- Staff are aware that Internet Traffic is monitored and traced to the individual user. Professional conduct is essential at all times.
- Staff that manage filtering systems and monitor the ICT use are supervised by senior management and have a clear procedure for reporting issues.
- Staff training in safe and responsible internet use and the school online safety policy is provided at least every two years.

28. How Parents Support is Enlisted:

Internet use in pupils' homes is increasing rapidly encouraged by offers of free access and continued media coverage. The school supports the parents by providing information to parents via the school website.

- Parents attention is brought to the Online Safety and Acceptable Use Policy in newsletters, and school website.
- Internet issues are handled sensitively and parents are advised accordingly.
- A partnership approach with parents is encouraged.
- Advice of filtering systems and educational leisure activities that include responsible use of the internet are made available to parents.
- Support resources on internet

29. Legal Framework:

Many young people and staff use the internet regularly without being aware that some of the activities that they participate in are potentially illegal. The law is developing rapidly and recent changes have been enacted through:

- The Sexual Offences Act 2003, which introduces new offences of grooming, and , in relation to making/distributing indecent images of children has raised the age of the child to 18 years old.
- The racial and religious hatred act 2006 which creates new offences which includes stirring up hatred against persons on religious grounds; and
- The Police and Justice Act 2006 which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.
- SLT and staff will regularly monitor the usage of the Learning Platform by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the Learning Platform.
- Only members of the current pupil, parent and staff community will have access onto the Learning Platform.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

Mobile Phones and Personal Devices

The use of mobile phones and personal devises is a school decision and the following points are in place:

- The use of mobile phones and other personal devices by pupils and staff in school will be decided by the school and covered in the School Acceptable Use Policy.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school Behaviour Management Policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school behaviour or bullying policy. The phone or device might be searched by the Senior Leadership Team with the consent of the pupil or parents. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the Police for further investigation.
- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.the school day.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such times. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Pupil Use of Personal Devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents in accordance with the school policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff, where necessary, will be issued with or can use a school phone where contact with pupils or parents is required.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

Racial and Religious Hatred Act 2006

The act makes it a criminal offence to threaten people because of their faith or to stir up religious hatred by publishing, displaying or distributing written material which is in anyway threatening.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the internet) It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

It is an offence for a person in position of trust to engage in sexual activity with any person under 18, with any person with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff).

GDPR:

- Data protection replaced by GDPR as of 25/05/2018
- School working with cyber essentials to certify compliance.
- School has an external DPO.
- Every effort is made to ensure all software and companies used are GDPR compliant.

Computer Misuse Act 1990

Regardless of an individual's motivation the Act makes it a criminal offence to:

- Gain access to computer software without permission, for example using someone else's password to access files.
- Gain unauthorised access as above in order to commit a further criminal act such as fraud.
- OR Impair the operation of a computer or programme, for example caused by virus or denial service attacks.

Malicious Communications Act 1998

This legislation makes it a criminal offence to send e-mails that convey indecent grossly offensive, threatening material or false information or is of an indecent or grossly offensive nature if the purpose of the e-mail was to cause the receiver to suffer stress or anxiety.

Copyright Design and Patents Act 1998

Copyright has the right to prevent others from using his or her work without permission. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence

Protection of Children Act 1998

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. The age of a child in this purpose is under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image.

Obscene Publications Act 1959 and 1964

Publishing an obscene article is a criminal offence. Publishing includes electronic transmission.

Disclaimer of endorsement

The information in this policy includes links or pointers to information created and maintained by other public and private organizations. St. George's Church of England Foundation School provides these links and pointers solely for our users' information and convenience. When users select an outside organisation, they are subject to the privacy and security policies of the owners or sponsors of the outside organisation, not St. George's Church of England Foundation School.

- St. George's Church of England Foundation School **does not** control or guarantee the accuracy, relevance, timeliness, or completeness of information of another website/organisation.
- St. George's Church of England Foundation School **does not** endorse the organisations sponsoring linked websites/organisations, and we do not endorse the views they express or the products or services they offer.
- St. George's Church of England Foundation School **cannot** authorize the use of copyrighted materials contained in linked websites/organisations. Users must request such authorization from the sponsor of the linked website.
- St. George's Church of England Foundation School **is not** responsible for transmissions users receive from linked websites/organisations.
- St. George's Church of England Foundation School **does not** guarantee that outside websites/organisations comply with Section 508 (accessibility requirements) of the Rehabilitation Act.

ST GEORGE'S CHURCH OF ENGLAND FOUNDATION SCHOOL

ACCEPTABLE USE

POLICIES (AUPs)

FOR BOTH STAFF AND PUPILS

"***For the body does not consist of one member but of many***" *1 Corinthians 12:14*

HOPE **FORGIVENESS** **COMPASSION** **FRIENDSHIP** **WISDOM**

NETWORK ACCEPTABLE USE POLICY (PUPILS)

This code of conduct applies at all times, in and out of school hours, whilst using school equipment. The Senior Leadership Team retain the right to amend these rules at any time. The new rules will be posted on the Intranet. Please read carefully:

1. **Network Requirements - All users must:**
   - 1.1 Respect all equipment; you will be charged for equipment damage, including labour fees.
   - 1.2 Make St George's IT Support Team aware immediately of any virus warning or threat.
   - 1.3 Respect copyright and trademarks. (Material cannot be copied without giving credit to the person or company that owns it).
   - 1.4 Read and adhere to the Acceptable Use Policy before using new technologies.
   - 1.5 Read, agree and adhere to any other Acceptable Use Policies as appropriate.
   - 1.6 Always seek staff permission before using a computer.
   - 1.7 Only use staff supervised areas outside lesson times.
   - 1.8 Monitor their user space and keep it below the limit, without wasting lesson time.
   - 1.9 Read and adhere to any local rules such as Sixth Form, Learning to Learn Centre and Library Resource Centre Acceptable Use Policies.

2. **Network Requirements - All users must not:**
   - 2.1 Use any other logon account other than their own.
   - 2.2 Use the Curriculum Network (or save files) for any other purpose which is not directly related to school work.
   - 2.3 Run any program not officially installed on the network, regardless of what it is for. Attempting to install any computer program is not allowed. Software requests must go via a member of St George's IT Support Team.
   - 2.4 Save files with either offensive contents or filenames. (Such files will be deleted regardless of content). File names over 255 characters will be periodically deleted.
   - 2.5 Send, access or display offensive messages or pictures.
   - 2.6 Attempt to hack, modify or infect the network using any program or virus.
   - 2.7 Deliberately attempt to install malicious software on any machine.
   - 2.8 Attempt to circumvent network security.
   - 2.9 Connect personal and non authorised devices to the network infrastructure without permission from a member of St George's IT Support Team.
   - 2.10 Damage or remove any school equipment.
   - 2.11 Use or send bad language.
   - 2.12 Intentionally waste resources thus preventing use by others.
   - 2.13 Eat or drink near any machine, or in any computer room.
   - 2.14 Play games or engage in other non curricular activities without permission from a member of staff.

3. **Additional Points:**
   - 3.1 Pupil user areas on the school network will be closely monitored and St George's IT Support Team may review files and communications to maintain system integrity. This also includes monitoring pupil activity remotely.
   - 3.2 Failure to follow relevant Acceptable Use Policies may result in loss of access and further disciplinary action may be taken if appropriate.
   - 3.3 If applicable, external agencies may be involved as certain activities could constitute a criminal offence.

Primary Pupils' Acceptable Use Policy

Year R and KS1:

- I only use the internet when an adult is with me.
- I only click on links and buttons when I know what they do.
- I keep my personal information and passwords safe online.
- I only send messages online which are polite and friendly.
- I know the school can see what I am doing online.
- I always tell an adult if something online makes me feel unhappy or worried.
- When I use an iPad or computer, I will only go on Apps or pages that my teacher has chosen.
- I know that if I do not follow the rules then I may not be allowed to use the iPads or computers for my learning.

- I have read and talked about these rules with my parents
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online

KS2:

- I know that I will be able to use the internet in school, for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to use the internet at school.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these I should report it to a teacher or adult in school or a parent or carer at home.
- I use my school computers and iPads for school work unless I have permission otherwise
- I will not use my own personal devices in school.
- I will not bring memory sticks or CD ROMs from home to use in school computers without my teacher's permission.
- I know that not everything or everyone online is honest or truthful and will check content on other sources like other websites, books or with a trusted adult
- I always credit the person or source that created any work, image or text I use
- I only talk with and open messages from people I know and I only click on links if I know they are safe
- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened.
- I will be polite and sensible when I message people online and I know that sending a message is the same as having a conversation with someone. I will not be rude or hurt someone's feelings online.
- I keep my personal information safe and private online.
- I will keep my passwords safe and not share them with anyone.
- I will not access or change other people's files or information.

- I will only post pictures or videos on the Internet if they are appropriate and if I have permission.
- I will only change the settings on the computer if a teacher/technician has allowed me to.

- I will not download software or files from the internet.
- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.
- I know that I am not allowed on personal e-mail, social networking sites or instant messaging in school.
- I know that my use of school devices/computers and Internet access will be monitored
- I know that if I do not follow the rules then my parents/carers will be informed and I may not be able to use the school iPads or computers for my learning.
- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page, shut the lid or turn off the screen and tell an adult straight away.
- If I am aware of anyone being unsafe with technology then I will report it to a teacher.

- I have read and talked about these rules with my parents
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online.

INTERNET ACCEPTABLE USE POLICY (PUPILS)

INTERNET USE IS FOR EDUCATIONAL BASED WORK ONLY.

1. **Internet Regulations - All users must:**

1.1 Be polite in any communications. Poor communication reflects on you and the School. Bad language will NOT be tolerated.
1.2 Respect Copyright and Intellectual property rights.
1.3 Adhere to any applicable laws, including the Computer Misuse and Data Protection Act, Copyright, Design & Patents Act and The Telecommunications Act.
1.4 Note that entering in to illegal or offensive activity is strictly banned (including sharing such information).

2. Internet Regulations – All users must not:

2.1 Use the Internet without supervision unless involved in private study. This does not apply to Sixth Form.
2.2 Use 'Proxy Avoidance' sites or attempt to get around the school's blocking/filtering systems.
2.3 Use 3rd Party webmail accounts such as Hotmail, GMail for communication. You have a 2.4 School email account if appropriate.
2.4 Use social sites such as Twitter, Facebook & Instagram, chat or Instant messenger programs and websites
2.5 Make purchases via shopping, auction or insurance sites.
2.6 Download or run any program which has not been authorised by the Network Manager.
2.7 Attempt to use Peer to Peer sites, Voice over Internet Protocol or any other unauthorised utility.
2.8 Download files such as executables, movies or music files (MP3s) unless authorised.
2.9 Share or forward any confidential information**.**
2.10 Attempt to set up any file sharing or web servers from within School.
2.11 Connect your own device (PC, phone, PSP etc) to the school network or Internet connection, without permission from a member of staff.

6TH FORM PUPILS ACCEPTABLE USE POLICY

1. **Network Regulations for Sixth Form Pupils:**

   1.1 You may use the Computer Facilities for School Work only.

2. **You are reminded that parts of the Network & Internet Acceptable Use Policies state that:**

   2.1 Playing games of any kind is forbidden unless for a curricular activity.
   2.2 Use of the Internet for anything other than school work is forbidden.
   2.3 Installing, attempting to install or running any computer programme that is not already installed on the Network is not allowed.
   2.4 Downloading of executable, movie and/or sound files are forbidden without the express permission from a member of St George's IT Support Team. Please be aware that you may not use the Sixth Form or Learning Resource Centre computers at lunchtime without permission from the staff within those Centres.
   2.5 Any loss, damage or vandalism to computer equipment will be charged directly to those concerned.
   2.6 You may not use social sites such as Twitter, Facebook, & Instagram, chat or Instant messenger programmes and websites
   2.7 Please also be aware that your use may be monitored at any time by members of staff.
   2.8 You must agree to and abide by all relevant Acceptable Use Policies (AUPs), e.g. Network, Internet and Email AUPs.

LEARNING RESOURCE CENTRE ACCEPTABLE USE POLICY (PUPILS)

1. **Network Regulations for pupils using the Learning Resource Centre:**

   1.1 You may use the Computer Facilities for School Work only.

2. **You are reminded that parts of the Network & Internet Acceptable Use Policies state that:**

   2.1 Playing games of any kind is forbidden unless for a curricular activity.
   2.2 Use of the Internet for anything other than school work is forbidden.
   2.3 Installing, attempting to install or running any computer program that is not already installed on the Network is not allowed.
   2.4 Downloading of executable, movie and/or sound files are forbidden without the express permission from a member of St George's IT Support Team.
   2.6 You must gain permission from staff before using the Internet (web/email).
   2.7 Any loss, damage or vandalism to computer equipment will be charged directly to those concerned.
   2.7 Please also be aware that your use may be monitored at any time by members of staff.
   2.8 You must agree to and abide by all relevant Acceptable Use Policies (AUPs), e.g. Network, Internet and Email AUPs.

EMAIL ACCEPTABLE USE POLICY (PUPILS)

1. **Email Regulations - All users must:**

   1.1 Agree to the Internet Acceptable Use Policy (rules), which covers any email activity which can be accessed through the Intranet.
   1.2 Agree to the Email Acceptable Use Policy which are as follows:
   1.3 Keep all communications polite, decent and within all rules.

2. **Email Regulations - All users must not:**
   2.1 Send any emails containing offensive, indecent or illegal matter to anyone, no matter if you know them or not.
   2.2 Attempt to transmit any viruses or illegal material. This is against the law and your details will be passed to the Police.
   2.3 Use your school email address or school facilities for mass email or for spamming.
   2.4 Impersonate any other person.
   2.5 Use any other account other than your own.
   2.6 Attempt to change any message headers.

3. **Additional Points:**
   3.1 If you are found to be emailing offensive content, you may be banned and/or contacted by a member of staff.
   3.3 The School reserves the right to view any sent or received emails.
   3.4 All incoming and outgoing emails are virus checked.
   3.5 If your email box becomes too large data may be deleted.

NETWORK AND INTERNET ACCEPTABLE USE POLICY (STAFF)

INTERNET USE IS FOR EDUCATIONAL BASED WORK ONLY.

1. Regulations of the School System

1.1 The Governing Board recognises that the ease of access and use of the Internet and all other ICT resources has resulted in it becoming a valuable source of information.

1.2 It should be noted that access to the Internet and all school electronic communication systems are made available to employees only to carry out the legitimate business of St. George's Church of England Foundation School.

1.3 All communications are subject to a review by appropriate and authorised personnel at any time and so users should have no expectation of personal privacy in the use of the School's communication systems or information sent to, from or stored in them.

1.4 No pupil mobile numbers should be held on any telephones by staff.

2. Acceptable use of ICT

2.1 It is not acceptable to access, try to access or circulate (email) any material which is, for example:

- Violent or which glorifies violence.
- Criminal, terrorist or which glorifies criminal activity (including drug abuse).
- Racist or designed to incite racial hatred.
- Content of extreme political opinion.
- Pornographic or with otherwise unsuitable sexual content.
- Crude, profane or with otherwise unsuitable language.
- In breach of the law, including copyright law, data protection and computer misuse.
- Belonging to other users of ICT systems and which they do not have explicit permission to access.

2.2 Staff must only modify, move or delete files within their own home directories. Users must not modify or delete files or programs not in their home directories without the explicit permission of the system administrator(s).

2.3 No pupil data to be held on C or Local Drives OF ANY SCHOOL COMPUTER, including laptops which may be taken off premises.

2.4 Staff must not delete, move or modify the existing structure of shared folders or areas.

2.5 Staff must not add or delete any software without prior permission from the Deputy Headteacher (Support).

2.6 CD writers in school should not be used for illegal copying of software.

2.7 Staff must not install, download or even try to download any software on to the network including individual computers on the network without express permission from the system administrator(s).

2.8 Staff have a responsibility to ensure that no Management Information Systems (i.e. Sims.net) are left running whilst their computer terminal is unattended at school or elsewhere.

2.9 Staff must be extremely cautious about revealing any personal details, and never to reveal a home address or telephone number, in communication.

2.10 Management Information Systems i.e. Sims.net can only be accessed by authorised members of staff and it is their responsibility when accessing confidential data that this data remains confidential.

2.11 Staff must not use other people's user IDs or passwords, even with their permission.

2.12 Staff should not allow pupils access to staff user areas.

2.13 These rules apply to all pupil use of the curriculum network. Support and technical staff have explicit exclusions from some rules.

3. Protection of School and User Rights

3.1 In order to protect responsible users, electronic methods will be used to help prevent access to unsuitable material. Any use of ICT including email may be monitored and recorded to ensure that this policy is followed.

3.2 Any such use of ICT equipment will be reported and investigated with disciplinary action being taken by the Governing Board if necessary.

3.3 The School will not accept that there are **any** circumstances where an individual may use unauthorised software on their stand-alone computers, laptops or network. Security is viewed seriously and any breach of this could lead to disciplinary proceedings.

3.4 Any deliberate use of unauthorised software which breaches the Copyright Law and Federation Against Software Theft (FAST), must be considered gross misconduct.

3.5 Staff need to be aware that the hardware, including laptops, is the property of the School and may be recalled at any time for maintenance, etc. This could lead to the loss of unauthorised applications or files which have been saved to the hard drive and not to the network.

Disclaimer of endorsement

The information in this policy includes links or pointers to information created and maintained by other public and private organizations. St. George's Church of England Foundation School provides these links and pointers solely for our users' information and convenience. When users select an outside organisation, they are subject to the privacy and security policies of the owners or sponsors of the outside organisation, not St. George's Church of England Foundation School.

- St. George's Church of England Foundation School **does not** control or guarantee the accuracy, relevance, timeliness, or completeness of information of another website/organisation.
- St. George's Church of England Foundation School **does not** endorse the organisations sponsoring linked websites/organisations, and we do not endorse the views they express or the products or services they offer.
- St. George's Church of England Foundation School **cannot** authorise the use of copyrighted materials contained in linked websites/organisations. Users must request such authorisation from the sponsor of the linked website.
- St. George's Church of England Foundation School **is not** responsible for transmissions users receive from linked websites/organisations.
- St. George's Church of England Foundation School **does not** guarantee that outside websites/organisations comply with Section 508 (accessibility requirements) of the Rehabilitation Act.

ST GEORGE'S CHURCH OF ENGLAND FOUNDATION SCHOOL

ACCEPTABLE USE RULES FOR STAFF

July 2015

"***For the body does not consist of one member but of many***" *1 Corinthians 12:14*

HOPE **FORGIVENESS** **COMPASSION** **FRIENDSHIP** **WISDOM**

St George's C of E Foundation School

Acceptable Use Rules for Staff

These rules apply to all on-line use and to anything that may be downloaded or printed.

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the Internet or E-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the Internet or send them via E-mail.
- I know that images of pupils are not to be taken on personal technical devices.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for children's or young people's safety to the Headteacher, Designated Safeguarding Lead, or online Safety Co-ordinator in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Safeguarding Officer is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail and should use the school E-mail and phones (if provided) and only to a child's school E-mail address upon agreed use within the school.
- I know that I should not be using the school system for personal use unless this has been agreed by the Headteacher and/or online Safety Co-ordinator.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will only install hardware and software I have been given permission for.
- I will ensure that I follow the Data Protection Act 1998 and the GDPR 2018 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the online Safety Co-ordinator.
- I have been given a copy of the Acceptable Use Policy to refer to about all online safety issues and procedures that I should follow.
- I will adhere to copyright and intellectual property rights.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of online Safety and my responsibilities to safeguard children and young people when using on-line technologies.

Signed: _____ Date: _____

Name _____

School: St. George's Church of England Foundation School

St George's C of E Foundation School
Acceptable Use Rules for Governors

These rules apply to all on-line use and to anything that may be downloaded or printed.

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the Internet or E-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I should never send inappropriate emails.
- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I know that images of pupils are not to be taken on personal technical devices.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for children's or young people's safety to the Headteacher, Designated Safeguarding Lead, or Online Safety Co-ordinator in accordance with procedures listed in the Acceptable Use Policy.
- I know who the Online Safety Co-ordinator is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, e.g. Facebook, Twitter or other Social Network sites, including my personal e-mail and should use the school E-mail and phones (if provided) and only to a child's school E-mail address upon agreed use within the school.
- I know that Social Media misuse will be treated in the same way as other misconduct.
- I know that I should not be using the school system for personal use unless this has been agreed by the Headteacher and/or online Safety Co-ordinator.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will only install hardware and software I have been given permission for.
- I will ensure that I follow the Data Protection Act 1998 and the GDPR 2018 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the Online Safety Co-ordinator.
- I have been given a copy of the Acceptable Use Policy to refer to about all online safety issues and procedures that I should follow.
- I will adhere to copyright and intellectual property rights.
- I know I must never post any videos regarding school on You Tube.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of online Safety and my responsibilities to safeguard children and young people when using on-line technologies.

Signed: _____ Date: _____

Name _____

School:St. George's Church of England Foundation School

SCHOOL'S ONLINE SAFETY AUDIT

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for online safety policy. Staff that could contribute to the audit include: Safeguarding Officer, SENCO, Network Manager and Headteacher.

Has the school an online Safety Policy that complies with Kent guidance?	**Y**
Date of latest update (November 2019):	
Date of future review (November 2020):	
The school online safety policy was agreed by Governors on (November 2019):	
The policy is available for staff to access at (School Website):	
The policy is available for parents to access at (School Website):	
The responsible member of the Senior Leadership Team is (Judy Wreford):	
The Governor responsible for online safety is (Teresa Carpenter):	
The Safeguarding Officer is (Judy Wreford):	
The online safety Co-ordinator is (Judy Wreford):	
Were all stakeholders (e.g. pupils, staff and parents) consulted with when updating the school online Safety policy?	**Y**
Has up to date online safety training been provided for all members of staff? (not just teaching staff).	**Y**
Do all members of staff sign an Acceptable Use Policy on appointment?	**Y**
Are all staff made aware of the schools expectations around safe and professional online behaviour?	**Y**
Is there a clear procedure for staff, pupils and parents to follow when responding to or reporting an online safety incident or concern?	**Y**
Have online safety materials from CEOP, Childnet and UKCCIS etc been obtained?	**Y**
Is online safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?	**Y**
Are online safety rules displayed in all rooms where computers are sued and expressed in a form that is accessible to all pupils?	**Y**
Do parents or pupils sign an Acceptable Use Policy?	**Y**
Are staff, pupils, parents and visitors aware that network and internet use is closely monitored and individual usage can be traced?	**Y**
Has an ICT security audit been initiated by SLT?	**Y**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y**
Is internet access provided by an approved educational internet service provider which complies with DfE requirements (e.g. KPSN)?	**Y**
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	**Y**
Are members of staff with responsibility for managing filtering, network access and monitoring systems and adequately supervised by a member of SLT?	**Y**
Does the school log and record all online safety incidents, including any action taken?	**Y**
Are the Governing Board and SLT monitoring and evaluating the school online safety policy and ethos on a regular basis.?	**Y**