Work together, Play together, Learn together…Shine
"Let your light shine" Matthew 5:16

St George's School, Bourton

Online Safety and Acceptable use of the Internet Policy

Author	Adoption Date	Review Date
Tom Abbott		

Document Name	Date of Issue	Date of Revision
Online Safety and Acceptable use of the Internet Policy	Autumn 2007	Spring 2017
		Autumn 2021

Online Safety Policy

Policy Contents:

1. Scope of this Policy

The internet has become an important aspect of everyday life, to which children need to be able to respond safely and responsibly. At St George's School, we believe that the internet offers a valuable resource for teachers and children, as well as providing new ways to communicate with others worldwide. At the same time there are risks that children may gain access to material that is inappropriate. This policy sets out the measures to be taken that minimises these risks.

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

This policy should be read in conjunction with other related policies and procedures:

- DFE Keeping Children Safe in Education (September 2021)
- DFE Teaching Online Safety in School (June 2019)
- UKCCIS Education for a Connect World (June 2020)
- St George's School Safeguarding and Child Protection Policy
- St George's School Behaviour Policy
- St George's School Staff Code of Conduct

Disclaimer

St George's School has made every effort to ensure that the information in this policy is accurate and up to date. If errors are brought to our attention, we will correct them as soon as is practically possible. However, St George's School cannot accept responsibility for any loss, damage or inconvenience caused as a result of reliance on any content in this publication.

2. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within St George's School:

2.1. Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Designated Safeguarding Governor receiving information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor and this role will include:

- Annual meetings with the Online Safety Co-ordinator,
- Annual update of incident monitoring,
- Reporting to the FGB.

2.2. Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher and DSL are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support for those in school who carry out the internal online safety monitoring role.

2.3. Online Safety Lead

The Online Safety lead is responsible for ensuring they:

- Lead Online Safety teaching across the school and reviews this regularly.
- Logs, tracks and monitors Online Safety Incidents.
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Provides an Online Safety training induction and shares the Online Safety Policy and Staff Acceptable Use policy with any new members of staff.
- Liaises with the Local Authority.
- Liaises with the Turn IT ON IT Team.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meets regularly with the Online Safety Governor to discuss current issues and review incident logs.

2.4. Technical Staff

"Turn IT ON" are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets online safety technical requirements and any Local Authority online safety policy/guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- That filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That monitoring software/systems are implemented and updated as agreed in school's Online Safety Policy

2.5. Teaching and Support Staff

Are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters.
- They have read and understood the school's Online Safety Policy and refer to it when needed.
- They have read, understood and signed the Staff Acceptable Use Policy.
- They report any suspected misuse or problem to the Online Safety Lead and/or DSL if it is also a safeguarding concern.
- All digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Teachers regularly engage students in Online Safety discussions as a response to any issues which may arise.
- Students understand and follow the Online Safety Policy and Children's Responsible Use of the Internet Policy.
- Students are taught research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies regarding these devices.
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

2.6. Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data,
- Access to illegal/inappropriate materials,
- Inappropriate online contact with adults/strangers,
- Potential or actual incidents of grooming,
- Child-sexual exploitation,
- Sexual violence and harassment,
- Sexting,
- Online-bullying.

2.7. Students

- Are responsible for using the school/academy digital technology systems in accordance with the Children's Responsible Use Policy (See Appendices).
- Will participate in teacher-led age-appropriate Online Safety Lessons.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies

on the taking/use of images and on online-bullying. See filtering and monitoring.

- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.

2.8. Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. St George's School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events,
- Access to parents' sections of the website,
- Their children's personal devices.

3 Education

'Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. We equip students with the knowledge needed to make the best use of the internet and technology in a safe, considerate, and respectful way so they are able to reap the benefits of the online world.' (DfE Keeping Children Safe in Education Annex C, p.96) We deliver online safety content within our curriculum and embed this within the wider whole school approach. 'From September 2020, Relationships Education is compulsory for all primary aged pupils, Relationships and Sex Education is compulsory for all secondary aged pupils and Health Education is compulsory in all state-funded schools in England. Through these new subjects, pupils will be taught about online safety and harms. This includes being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives.' (DfE Teaching Online Safety in School p.5).

3.1 Education for Pupils

Whilst regulation and technical solutions are especially important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

3.1.1. Planning for Online Safety

At St George's School we have a progressive curriculum based on the Rising Stars "Switched on Computing" scheme of work. Our computing curriculum will cover the principles of online safety at all key stages, with progression in the context to reflect the different risks that pupils face. This includes, 'How to use technology safely, responsibly, respectfully and securely and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.' (DfE Teaching Online Safety in School p.5).

Our students have planned Online Safety sessions within our Computing Curriculum. Online Safety is being explicitly taught throughout the year in small but frequent chunks. The sessions focus on a range of areas of Online Safety, including sessions specifically linked to the potential risks outlined in the Teaching Online Safety in Schools document (2020). Each session focuses on a different strand of Online Safety and an overview can be seen below:

	Internet Safety	Privacy and Security	Relationships and communication	Cyberbullying	Self-image and Identity	Information Literacy	Creative Credit and Copyright
FS	✓	✓	✓			✓	
1	✓	✓	✓			✓	✓
2	✓	✓	✓		✓	✓	
3	✓	✓	✓	✓		✓	
4		✓		✓	✓	✓	✓
5	✓	✓			✓	✓	✓
6	✓	✓		✓	✓	✓	

From these Online Safety Sessions, teachers then refer to them throughout the year. If more sessions are needed, these can also be embedded in other curriculum areas and class discussions.

3.1.2. Vulnerable Pupils and SEND

Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstance. However, there are some pupils, for example looked after children (LAC) and those with special educational needs (SEND), who may be more susceptible to online harm or have less support from family or friends in staying safe online.

Our School recognises the additional risks that children with SEN and disabilities face online. To help protect our most vulnerable we:

- Continue to raise awareness of Online Safety towards all members of our school community.
- Develop a route to identify those more at risk.
- Support learners through open conversation.
- Ensure that staff are effectively trained to identify our most vulnerable and recognise the addition risks vulnerable children face online.
- Involve key agencies where necessary.
- Establish a process to increase learner awareness and monitor needs.

3.1.3. Other Curriculum Links

In addition to specific, planned Online Safety sessions, there are opportunities to teach pupils how to use the internet safety in other curriculum areas. Our PHSE Curriculum follows the SCARF Scheme which also covers different aspects of Online Safety within these sessions.

For EYFS and Key Stage One, the PHSE linked to Online Safety focuses on relationships, bullying and self-identity. All are contributing factors to consider when looking at Online Safety. For Key Stage Two, there are in addition specific sessions on online safety such as Online Gaming and Gambling, Sexting, Cyberbullying and Exploitation (such as 'County Lines' and gang culture).

Each February we also celebrate Safer Internet Day as a whole school. We have sessions dedicated to Online Safety for the children and lead collective worships to raise awareness of Online Safety. This is also a time when the school measures the impact of Online Safety. Children and parents complete a questionnaire relating to their Online Safety teaching. The Online Safety Lead analyses the results from this questionnaire to inform their action plan and put in additional measures and support where needed.

If an Online Safety incident arises in a specific class, or there is a concern/questions raised by a child in a specific class. Teachers will address these concerns/questions as it emerges through positive class discussion. This will also enable a culture of open talk within classes.

We also support students in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. This is encouraged discussion through our teaching of British Values, SMSC, RSE and PHSE as well as through Online Safety sessions in computing.

As of September 2020, relationships and sex education (RSE) is mandatory. The government guidance states, 'In primary schools, we want the subjects to put in place the key building blocks of healthy, respectful relationships, focusing on family and friendships, in all contexts, **including online**.' (DfE Relationships and Sex Education 2020). The DfE's RSE Curriculum states what the pupils should know by the time they leave primary school. As a school, the statements from the RSE Curriculum are planned into our age-appropriate Online Safety Curriculum and additionally in our PHSE Curriculum.

The RSE DfE document statements linked to Online Safety states that pupils should know:

- About different types of bullying (including cyber bullying)
- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

3.2. Education for Parents and the Wider Community

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website, E-Schools
- Parents/carers information evenings
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant websites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers

4. Training

'Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 84) and the requirement to ensure children are taught about safeguarding, including online safety (paragraph 87), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.' (Keeping Children Safe in Education, Annex C, p98).

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- Evidence of Online Safety training is recording alongside other safeguarding training.
- All new staff receive online safety training as part of their safeguarding induction programme, ensuring that they fully understand the school's safety policy and Responsible Use Policy.
- The Online Safety Lead will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Lead will provide advice/guidance/training to individuals as required.
- The Governor responsible for safeguarding will be invited to attend any staff training and parent information evenings and will be regularly kept up to date by the Online Safety Lead.

5. Technical

5.1. Filtering and Monitoring

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Information received via the web, e-mail or text message requires good information-handling and digital literacy skills. It may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read.

Ideally inappropriate material would not be visible to pupils using the internet, but this is not easy to achieve and cannot be guaranteed. Pupils are taught what to do if they experience material that they find distasteful, uncomfortable, or threatening.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- Requests for filtering changes are managed/approved by SWGL.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The IT Team/Network Administrator regularly monitors and records the activity of users on the school technical systems.

- Specific lessons are included within the Computing/Online Safety scheme of work and PHSE/RSE lessons that teaches all pupils how to read for information from web resources.
- Older pupils are taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place (Community Users Responsible Use Agreement) for the provision of temporary access of guests (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place (Staff Acceptable Use Policy) regarding the extent of personal use that users (staff) are allowed on school devices that may be used out of school.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

6. Mobile Technologies

Mobile devices refer to any device that provides access to the internet or internal network for example, tablet (Apple Android, Windows, and other operating systems) e-readers, mobile phone, iPad, iPod touch, digital cameras and Smart Watches. Due to the widespread use of personal devices it is essential that schools take steps to ensure mobile devices are used responsibly and that they do not impede teaching and learning.

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes	Yes	No*	Yes**	Yes***
Full network access	Yes	Yes	Yes	No	No**	No

* Student Owned devices must be kept in the school office and parental permission is sought.

** Staff Owned devices are allowed in school but must adhere to the Staff Responsible Use Policy.

*** Visitors (e.g. Healthcare providers) are allowed devices in school but permission from a member of the Senior Leadership Team is sought.

- Personal mobile devices (including mobile phones, smart watches and tablets) are not to be brought into school by pupils and the school accepts no responsibility for the loss, theft or damage of such items should they bring into school.
- In extenuating circumstances, mobile phones may be brought in where parents have specifically requested for use regarding contact arrangements etc. but MUST be handed to the school office at the beginning of the day to be kept securely in the office.
- Staff use of mobile devices should follow the points set out in the Staff Acceptable Use Policy and Staff Code of Conduct.
- School staff, authorised by the Headteacher, may search pupils or their possessions, and confiscate any mobile device which they believe to contravene school policy, constitute a prohibited item, is considered harmful, or detrimental to school discipline. If it is suspected that the material contained on the mobile device relates to a criminal offence, the device will be handed over to the Police for investigation.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour policy. 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.
- Where staff may need to contact children, young people and their families within or outside of the setting in a professional capacity, they should only do so via an approved school account (e.g. e-mail, phone).
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community.
- Staff should be provided with school equipment for the taking photos or videos of pupils linked to an educational intention. In exceptional circumstances staff may need to use personal devices for such a purpose and when doing so, should ensure they comply with the Staff Code of Conduct, Staff Responsible Use Policy and seek permission from the Headteacher.
- Staff may use their own mobile phones for emergency use on school trips providing they comply with the Staff Code of Conduct, Staff Responsible Use Policy and seek permission from the Headteacher.
- Appropriate use of mobile phones will be taught to pupils as part of their PSHE and Online Safety programme.
- For the safeguarding of all involved, users are encouraged to connect mobile devices through the school wireless provision and service that allows the ability to filter any device that uses the school internet connection, without having to configure the user's device.
- Mobile phones will not be used by staff during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from the Headteacher.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

7. Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However along with the significant benefits there are also significant risks. The school will inform and educate users about risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images through Online Safety teaching.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/newsletters/social media/local press.
- Class teachers are provided with an updated list of photo permissions and these are kept in classroom at all times.
- Pupils' full names are not used anywhere on the website, particularly in association with photographs.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school/academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims but must follow the school's Staff Acceptable Use Policy.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Individual class pages (homepage) are only accessible to parents of a child in that class via individual logins and children within their own class.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

8. Data Protection

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 2018 (GDPR) gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Schools will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.

For advice and guidance relating to a contravention of the Act, contact Dorset council guidance for schools.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

9. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

9.1. E-mail / TEAMS

- Pupils may only use e-school messaging to communicate with staff and should not have access to personal email accounts within school.
- Pupils must follow the guidance set out in the children's Responsible Use Policy.
- Staff will monitor message threads between children within their class and any children who are not following the guidance set out in the children's Responsible Use Policy will face appropriate consequences set out in the school's Behaviour Policy, this may include: reminders from the class teacher or Online Safety Lead, loss of access to e-schools, phone calls home etc.
- E-Schools will flag up any messages reporting abuse and staff will be sent a notification.
- Pupils must immediately tell a teacher if they receive offensive messages.
- Staff must comply with the Staff Code of Conduct, Staff Responsible Use Policy and Data Protection Policy when engaging in any correspondence using school email accounts.
- Staff must use official school provided e-mail accounts for all professional communications.
- Abusive messages towards staff will not be tolerated and if staff feel they have received an abusive message from a parent, child or another member of staff must inform the Headteacher immediately.
- Sending images without consent or messages that cause distress and harassment to others are considered significant breaches of school conduct.

9.2. Social Media

Online communications, social networking and social media services are filtered in school by their ISP but are likely to be accessible from home.

All staff have been made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally as set out in the Staff Acceptable Use Policy and Staff Code of Conduct. They are aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. St George's School actively encourages pupils about the importance of keeping personal information safe.

- Pupils should not have access to social media when in school.
- Pupils are taught how to keep personal information safe when using online services. Examples include: real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils must not reveal personal details of themselves or others in online communication, or arrange to meet anyone.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private. This is in line with the school's online safety teaching scheme of work.
- No member of the school community should publish specific and detailed private thoughts about the school, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites will be raised with their parents/carers, particularly when concerning students' underage use of sites. Any concerns about a pupil's welfare will be raised with the school's designated safeguarding lead in accordance with the school's Safeguarding Policy.
- Staff personal use of social networking, social media and personal publishing sites (in or out of school) will be discussed as part of staff induction and safe and professional behaviour will be outlined in the Staff Acceptable Use Policy and the Staff Code of conduct.
- Staff communication on Microsoft Teams (or any other online communication between staff) will be for professional purposes and in line with staff professional communication behaviour outlined in the Staff Acceptable Use Policy.
- In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' it will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites.
- The computing co-ordinator will conduct annual pupil surveys about their home use of ICT. It will gauge the range of activities which pupils undertake and how safely they are using them, e.g. keeping personal information safe, experiences of cyber bullying etc.
- Additional guidance for staff is outlined in the Staff Responsible Use Policy.

10. Dealing with Incidents

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity report immediately to the police.

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school's policy. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with following our school's Behaviour Policy. Examples of student incidence and appropriate actions are listed below:

Student Incident:	**Actions:**							
	Refer to class teacher	Refer to DSL	Refer to Headteacher	Refer to IT Support	Inform parents/carers	Removal of access	Warning	Further consequences e.g. exclusion
Deliberately accessing or trying to access material considered to be illegal		X	X	X				
Unauthorised use of noneducational sites	X					X		
Unauthorised use of personal mobile devices	X				X			
Unauthorised use of social media	X			X	X	X		
Corrupting or destroying the data of others			X		X	X		
Sending an email, text or message regarded as offensive, harassment or of a bullying nature		X	X		X		X	

Continued infringements of above			X		X		X	X
Actions which could bring the school into disrepute			X		X			
Using proxy sites or other means to subvert the school's filtering systems	X			X			X	

- All record of the incident should be kept, e.g. e-mails saved or printed, text messages saved etc. Complaints of a safeguarding nature must be dealt with in accordance with Child Protection and Safeguarding Policy.
- Responsibility for handling incidents will be given to the Headteacher, including any complaint about staff misuse.
- The Online Safety Lead will keep a record of all incidents and regularly review them.
- The Online Safety Lead will regularly inform the Headteacher and DSL about any incidents.
- The facts of the case will need to be established, for instance whether the internet use was within or outside school.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaint's procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

11. Safeguarding and Child Protection

The use of technology has become a significant component of many safeguarding issues. The Department of Education's Keeping Children Safe in Educations (2021) Documents outlines that:

'The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:
Content: being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views;
Contact: being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults;
Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying.'

As a result of this, if an incident regarding online safety also raises concerns about the welfare of a child, the school will be following through with its safeguarding procedures following the school's Safeguarding and Child Protection Policy.

Draft - composed September 2021.

Finalised policy ratified at Governor Curriculum and Pastoral Committee Meeting:

Policy Written by Mr T Abbott

12. Appendices

1. St George's School, Bourton Acceptable Use Policy of ICT
2. Staff Responsible Use Agreement

St George’s School, Bourton
Acceptable Use Policy of ICT

1. Pupils must obtain the permission of parent(s)/guardian(s) before they can be allowed to use the Internet or education Email service. The Parental Permission Form must be signed and returned to the school.
2. Pupils should only use the school computer systems for those activities and services (Internet, Email and software) which they have been given permission.
3. Pupils must only use the school computers with the permission and under the instruction of a member of staff.
4. Activities that use the Internet during taught lessons will be directly related to school work. Use of the Internet outside of taught lessons is at the discretion of a member of staff who will set guidelines and rules for its use, in accordance with the existing school ICT policy.
5. Pupils must only use the user name and password that they have been given.
6. All users should not download material or copy and paste material which is identified as copyright.
7. All users have a responsibility to inform the member of staff supervising them and then that member of staff will complete an incident report if unsuitable materials (see footnote below) are accessed.
8. Pupils will be taught to respect the privacy of files and work of other users. They will be taught not to enter, attempt to enter or alter without permission the files areas or content of pupils or members of staff.
9. No external drive that can be brought in from home is to be downloaded onto the school network.
10. Where pictures of people are used on the website, full identification will not be given. Photographs of children will not be published without prior parental permission.
11. Pupils will not create or publish materials in school or home learning tasks which contain unsuitable materials. The choice of materials and resources used are the responsibility of the author. Non-compliance may result in legal action.
12. All users of ICT facilities will show respect for the equipment and for all individuals.

Failure to comply with this policy will result in one or more of the following:
A ban - temporary or permanent, on the use of the internet at school.
A letter - informing parents of the nature and breach of rules.
Legal action -

- In violation of any law or regulation
- Which is defamatory, offensive, racial, abusive, indecent and obscene.
- Which constitutes harassment
- Is in breech of confidence, privacy, trade secrets
- Is in breech of any third party Intellectual property rights (including copyright)
- Is in use of other rights or has any fraudulent purpose of effect.

Parental Permission for Pupils use of Internet Facilities at School

St George’s School has a connection to the Internet that provides a number of important and valuable contributions, enhancing learning and understanding in all of the school curriculum areas. Thousands of schools across the world now have access to the Internet, and many pupils and students are reaping the educational benefits this learning resource provides.

As a result of the open and unregulated nature of the Internet, there is some material that is unsuitable for viewing by children. Therefore, we have procedures that should enable your child to use the Internet facilities safely and securely. A copy of the school’s Acceptable Use Policy is on the reverse of this form. We will make every effort to ensure that unsuitable material is not viewed by your son/daughter. A member of staff will monitor each session. Each member of staff and parents of each pupil using the Internet must agree to the Acceptable Use Policy. This policy sets out the rules that must be adhered to, for the protection of all users within the school.

For your information the following web sites provide further information on ‘Safety on the Internet’:

https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis
(The UK Government Internet Safety site.)
http://www.iwf.org.uk (The Internet Watch Foundation website.)

The form below must be completed, signed and returned to the school for our records. The use of the Internet and/or e-mail service will be withheld unless this has been done.

I have read, understood and explained the Acceptable Use Policy to my child:

Pupil Name (PLEASE PRINT) …………………………………….……….. of ………… Base

Name of Parent/Guardian/Carer (PLEASE PRINT) ………………………………………….

Signature of Parent/Guardian/Carer ……………………………………. date …………….

Please indicate the services you will allow you child to use:

Service:	Signature of Parent/Guardian/Carer
The Internet (filtered access via industrial standard filtering)	
A filtered educational e-mail service	

St George's School

Staff Responsible Use Agreement

Please complete, sign and return to TFA

Full name:	
Role:	

This agreement has been written in line with St George's School Online Safety policy to ensure that all staff are up-to-date with the policies regarding Responsible Internet Use.

Please fill out the following form and hand back to Mr Abbott. (Computing and Online Safety Co-Ordinator).

I confirm:

- I have read and agree to the terms outlined in the Online Safety and Acceptable Use of the Internet Policy,
- I have read and agree to the terms outlined in the Staff Responsible Use Policy
- I have read and agree to the terms outlined in the Staff Code of Conduct,
- I have read and agree to the school's Safeguarding and Child Protection Policy.

Signed:	
Date:	