



St Catherine's Online Safety Policy

Schedule for Development / Monitoring / Review

This online safety policy was approved by the Governing Body	
The implementation of this online safety policy will be monitored by the Online safety Group:	Headteacher, Online safety Coordinator and Online safety Governor
Monitoring will take place at regular intervals:	December / June - yearly
The Governing Body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	July - Yearly
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	December 2016
Should serious online safety incidents take place, the following external persons / agencies should be informed:	
The School will monitor the impact of the policy using:	Logs of reported incidents <ul style="list-style-type: none">• monitoring logs of internet activity (including sites visited)• surveys / questionnaires of<ul style="list-style-type: none">• pupils• parents / carers• staff

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing its effectiveness.

- regular meetings with the Online Safety Co-ordinator, via the online safety group
- regular monitoring of online safety incident logs, via the online safety group
- regular monitoring of filtering / change control logs, via the online safety group

Headteacher:

- 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 Co-ordinator.
- 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 / Principal / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Online Safety Coordinator:

- 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
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets with online safety group to discuss current issues, review incident logs and filtering / change control logs

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 on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Network Manager / Technical staff:

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority / other relevant body Online safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Online safety Coordinator for investigation / action / sanction

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy
- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher / Online safety Coordinator
- 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
- that pupils understand and follow the online safety and acceptable use policies
- that pupils have a good understanding of 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 with regard to these devices
- in lessons where internet use is pre-planned students / pupils 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
- Have read the guidelines for the use of social media both in and out of school.

Students / pupils:

- Have read, understood and signed the 'Acceptable Use Policy' for their age group.

Parents / Carers

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 / VLE and on-line pupil records

Education

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety 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.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited including the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students / pupils 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

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. The school will take every opportunity to help parents understand these issues through newsletters, website / VLE and information about national / local online safety campaigns / literature.

Staff / Volunteers

- 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.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.

Governors

Governors should take part in online safety training / awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

Technical

Infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher / Principal or other nominated senior leader and kept in a secure place
- The Headteacher is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- 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. If a user requires a change to the filtering list they must approach the ICT Subject Leader who will meet with the Headteacher to approve / disapprove with the request.
- Actual / potential technical incident / security breach should be reported to the ICT Subject Leader or Headteacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programs on school devices.
- Users should not use their own removable media on school machine unless prior approval has been agreed. School machines are protected via the academies own antivirus software which should remove known malware and viruses. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Bring Your Own Device

- Currently all equipment is provided by the school.

Cyber Bullying

- Refer to the Bullying Policy

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- 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 events for their own personal use (as such use is 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 / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
Photographs will only be published on the school website with the permission of the parent/carer. We will only use pictures that included at least two children and will only be accompanied by the pupil's first name.
Photographs will only be published in newspapers with the permission of the parent/carer and will only include the pupil's first name. (See parent permission letter under attachments)

Data Protection

Refer to the Data Protection Policy

Communications in school

Communication Technologies	Staff		Pupils
	Allowed	Allowed at break / lunchtimes	Allowed
Mobile phones may be brought to school	✓	✓	X
Taking photos on personal mobile phones / cameras.	✓ with permission from the online safety coordinator or headteacher		X
Use of other personal mobile devices eg tablets, gaming devices	✓ with permission from the online safety coordinator or headteacher		X
Use of personal email addresses in school, or on school network		✓	X
Use of school email for personal emails	X	X	X
Use of messaging apps	X	✓	X
Use of social media / blogs	X	X	X

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the Online safety coordinator or headteacher the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school

systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above could be provided with individual school email addresses for educational use.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions

		Acceptable	Acceptable at certain times	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978				X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.				X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008				X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986				X
	pornography			X	
	promotion of any kind of discrimination			X	
	threatening behaviour, including promotion of physical violence or mental harm			X	
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute			X		
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / school				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming			✓		
On-line gambling				X	
On-line shopping / commerce			✓		
File sharing			✓		