St Nicholas CE First School Online Safety Policy

Reviewed January 2020 by Mr R Gough

Related Legislation:

Computer Misuse Act (1990)

Data Protection Act (1998)

The Equality Act 2010

Related School and Academy Trust Policies and Procedures:

St Nicholas' CE First School Anti-Bullying Policy

St Nicholas' CE First School Behaviour Policy

St Nicholas' CE First School Network Security Policy

St Nicholas' CE First School Prevent Policy

St Nicholas' CE First School Safeguarding Policy

Codsall Multi-Academy Trust Data Protection Policy

Related Guidance:

Department for Education: Keeping children safe in education (2018)

Department for Education: Working together to safeguard children

Department for Education: The Prevent Duty

General Data Protection Regulation

What is Online Safety?

Even though online services and associated technologies are an excellent tool and resource to enrich learning, there are still dangers related to their use, especially in relation to young pupils. Some examples of this are:

- Bullying via digital communication
- Obsessive internet use
- Exposure to inappropriate materials
- Inappropriate or illegal behaviour
- Physical danger of sexual abuse

Online safety consists of all the practices, precautions, preventative measures and procedures that ensure users of digital devices at St Nicholas CE First School are not accidentally or delibaretly accessing or being exposed content that either inappropriate and/or illegal. As a school it is our duty of care alongside that of parents and other members of the community to protect our children from these dangers and this can be achieved by many different mechanisms working together.

The purpose of this online safety policy is to outline what measures the school takes to ensure that students can work in a digitally safe environment and that any online safety issue is detected and dealt with in a timely and appropriate fashion.

At St Nicholas CE First School, we aim for preventative eduation by equipping our school community with the necessary knowledge, understanding and skills to prevent any issues arising from using technology.

In accordance with statutory guidance (Keeping Children Safe in Education: 2018), the issues that we aim to prevent are linked to three main areas of risk:

Content: being exposed to illegal, inappropriate or harmful material

Contact: being subjected to harmful online interaction with other users

Conduct: personal online behaviour that increases the likelihood of, or causes, harm

SEND and Dyslexia Friendly Schools' Policy Statement

At St. Nicholas First School, all pupils are valued equally. Teachers plan lessons which enable all pupils to participate, achieve and excel, whatever their level of ability. Lessons provide opportunities for pupils to recognise and develop their own learning style, (auditory, visual or kinaesthetic), through varied and flexible provision across a broad and balanced curriculum.

In order to meet the needs of all our pupils, we hold the Schools' Dyslexia Friendly Full Status.

Scope of this Policy

This document is intended for the general public as well as that of school members, parents and local community and is a clear outward statement on the school's online safety practices. This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school's digital systems, both in and out of the school. The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

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 governor(s) receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body (Safeguarding) will:

- Regularly meet with the Headteacher and Computing Leader
- Regularly meet with the school's online safety and digital pupil representatives

- Report on the implementation and effectiveness of this policy and any online safety initiatives to governors
-

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 Computing Leader. 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 is responsible for ensuring that the relevant individuals receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. 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. The Senior Leadership Team will receive regular monitoring reports from the Computing Leader.

The **Computing Leader** (Mr R Gough) is the named member of staff, who will oversee day to day responsibility for Online Safety, who will work closely alongside the Designated and Deputy Safeguarding Lead, in relation to any online safety incidents. The Computing Leader will also establish and review policies and procedures for monitoring and managing online safety awareness and incidents. They will also ensure that they regularly monitor the online monitoring system (Policy Central Enterprise) and record online safety recorded violations, regardless of whether they are genuine or false-positives. Reports such as this are kept within a password-protected digital record, which is accessible by both the Computing Leader and the Headteacher. Moreover, the Computing Leader will also liaise and provide detailed updates to the relevant governors and members of the leadership team.

Mr R Gough is EPICT (European Pedagogical ICT Licence) accredited and is a CEOP Ambassador. Therefore, he is equipped to deliver online safety training and awareness to members of and outside of the school community. For example, as part of Year 4 transition to Middle School, pupils participate in a range of preventative education activities, at a time when they are becoming increasingly independent.

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 and practices
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement
- (AUP)

- They report any suspected misuse or problem to the Headteacher and Computing Leader for investigation
- All digital communications with pupils and 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
- Pupils understand and follow the Online Safety Policy and acceptable use policies
- They monitor the use of digital devices 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, 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

Our network is managed by Concero Technology Services. Individuals at Concero are our **Network Management Staff**, who are responsible for ensuring:

- That the school's technical infrastructure is secure and not at risk to misuse or malicious attack.
- That the school meets required online safety technical requirements and any other 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.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- 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 digital network, online services and communication services are regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and Computing Leader for investigation.
- That monitoring software / systems are implemented and updated as agreed in school policies.

The **Designated Safeguarding Lead (Miss J Parker, Headteacher) and Deputy Safeguarding Leads (Mrs S Robb and Miss S Pugh, Assistant Headteachers)** 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
- Cyberbullying

Students are responsible for:

Using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement.

Ensuring they have an awareness and understanding of the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Understanding 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.

Parents/Carers play a crucial role in ensuring that their children understand the need to use online services and digital devices in an appropriate way. Research shows that many parents do not fully understand the issues and are less experienced in the use of digital services than their children. The school will therefore take every opportunity to help parents understand these issues through workshops, newsletters and the school website, in addition to I information about national/local online safety campaigns/literature.

The key responsibilities for parents are to:

- Support the school in promoting online safety which includes the pupils' use of online services and the school's use of photographic and video images
- Consult with the school if they have any concerns about their children's use of technology
- Ensure that they themselves do not use online services or other forms of technical communication in an inappropriate or defamatory way
- Support the school's approach to online safety by not uploading or posting online any pictures, video or text that could upset, offend or threaten the safety of any member of the school community or bring the school into disrepute.

Members of the wider school community who access the school's digital systems are expected to sign a 'Visitor Acceptable Use' policy. Failure to do so will result in access to the school's digital systems being denied.

Policy Statements

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
- Key online safety messages should be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials/ content they access online 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 supported 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. Additional duties for schools under the Counter Terrorism and Securities Act 2015 requires schools to ensure that children are safe from terrorist and extremist material online
- Pupils should be helped to understand the need for Acceptable Use Policies 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
- In lessons where online use is pre-planned, it is best practice that 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 online searches
- Where pupils are allowed to freely search online, staff should be vigilant in monitoring the content of the websites the young people visit

Education (Parents/Carers)

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 on-line behaviours. Parents/carers 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
- Digital Leaders
- High profile events/campaigns
- Reference to relevant web sites/publications

Education and Training (Staff and Volunteers)

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.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Computing Leader will receive regular updates through attendance at external training events 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 / INSET days.
- The Computing Leader will provide advice /guidance / training to individuals as required.

Education and Training (Governors)

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology, online safety, health and safety and safeguarding. 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 (this may include attendance at assemblies / lessons).

Technical Infrastructure, Equipment, Monitoring and Filtering

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:

School digital systems will be managed in ways that ensure that the school meets recommended technical requirements

• There will be regular reviews and audits of the safety and security of school

technical systems

• Servers, wireless systems and cabling must be securely located and physical access restricted

• All users will have clearly defined access rights to school digital systems and devices.

• All users will be provided with a username and secure password by Concero Technology Services, who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password on a regular basis.

• The Administrator passwords for the school digital system, used by Concero Technology Services must also be available to the Headteacher or other nominated senior leader and kept in a secure place

• Online access is filtered for all users.

Illegal content 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.

There is a clear process in place to deal with requests for filtering changes

• Online filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.

• School staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

• An appropriate system is in place for users to report any actual /potential technical incident / security breach to the relevant person, as agreed.

• 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 (to be described) for the provision of temporary access of "Visitors" (such as trainee teachers, supply teachers) onto the school systems.

• An agreed policy is in place regarding the extent of personal use that users are allowed on school devices that may be used out of school.

General Data Protection Regulation (GDPR)

St Nicholas CE First Scholl will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

The school and its employees will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

● Personal information about members of the school community – including pupils, members of staff and parents / carers, such as names, addresses, contact details, legal guardianship contact details, health records, disciplinary records

● Curricular / academic data e.g. class lists, pupil / student progress records, reports, references

● Professional records e.g. employment history, taxation and national insurance records, appraisal records and references

● Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Good practice suggests that all users will use strong passwords made up from a combination of simpler words. User passwords must never be shared. Personal data may only be accessed on machines that are securely protected. Any device that can be used to access personal data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation. Personal data should only be stored on school equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school personal data. When personal data is stored on any portable computer system, USB stick or any other removable media:

● The data must be encrypted and password protected

● The device must be password protected

● The device must offer approved virus and malware checking software

● The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

The school should have clear policy and procedures for the use of "Cloud Based Storage Systems" (Microsoft Office 365) and is aware that data held in remote and cloud storage is still required to be protected in line with GDPR. As a Data Controller, the school is responsible for the security of any data passed to a "third party".

School Initiatives

St Nicholas has a group of pupil representatives (Digital Leaders) within and across the school. They are responsible for raising and promoting awareness of online safety to the school community. In conjunction with this, the school also has a Digital Hero (designed by the children), which acts as a child-friendly and familiar character that supports in developing pupils' knowledge and understanding of online safety issues and how to deal with them. Furthermore, Digital Leaders regularly meet with Mr R Gough, Miss J Parker (Headteacher), governors and representatives from technology businesses. The Digital Leaders also regularly communicate to the whole and wider school community through the Digital Hero's Diary, which increases awareness through stories, hints and tips.

Monitoring of Digital Systems

St Nicholas CE First School has a highly efficient and effective digital monitoring system (PCE Console). Once a suspected violation has occurred, this captured on-screen, along with details such as: Username, Date, Time, IP address and Device, in addition to other information, which may include the name of the website or document. These violations are monitored throughout the week and a record is kept in the Network Monitoring Record of

the number of violations and action taken. Should any violations cause concern, these are referred to the appropriate safeguarding members of staff, who will decide on the most appropriate (and disciplinary, if necessary) action. See **'Responding to Incidents of Misuse' for further information'.**

Mobile Devices

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to online services which may include the school's website and other cloud based services such as email and data storage. All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

The school Acceptable Use Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies

The school allows:

	School Managed Devices		**Personal Devices**		
	School-owned device	**Authorised device**	**Student**	**Staff**	**Visitor**
Allowed in school	YES	YES	NO	YES (User must agree to AUP)	YES (User must agree to AUP)
Full network access (including online)	YES	YES (User must agree to AUP)	NO	YES (User must agree to AUP)	This is dependent on requirements
Online access	YES	YES (User must agree to AUP)	NO	YES (User must agree to AUP)	YES (User must agree to AUP)

Personal Smart Devices

For the purpose of this policy, a smart device may consist of any wearable or usable digital device that has the ability to take photos, videos, audio recordings and/or make phone calls or text messages across a network. The following applies to all staff and visitors to the school. Students are not permitted under any circumstances to wear or use personal smart devices on school premises.

Personal smart devices that are capable of taking photos, videos and recordings must not be used to digitally record any aspect or member of the school community

or record any discussions; they must never be used in the presence of children. Furthermore, personal smart devices that are capable of sending or receiving phone calls or text messages must only be used in a designated area, if absolutely necessary.

Personal smart devices are not allowed to be connected to the school's network and must not be used to access or view illegal or inappropriate content at any time, regardless of any external network (i.e. 4G/Cellular) that they are connected to, and must be silenced and disabled in 'Airplane Mode' until in a designated area.

Use of Digital Images and Clips

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded online. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images online. Such images may provide avenues for cyberbullying to take place. Digital images may remain available online forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out online searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

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 online

Written permission from parents or carers will be obtained before photographs or digital clips of pupils are published on the school website or any other online service

To respect everyone’s privacy and in some cases protection, digital images and clips of school events should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital images and clips.

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 published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Pupil's work can only be published with the permission of the pupil and parents or carers.

Communication

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff	Pupils
Mobile phones may be brought to the school	**Yes, yet they must be locked away securely**	**NO**
Use of mobile phones in lessons	**NO**	**NO**
Use of mobile phones in social time	**Only in a designated secure area away and out of sight of any pupil**	**NO**
Taking photos on mobile devices	**NO**	**Yes, for education use only on a school-owned device**
Use of other mobile devices e.g. tablets, gaming devices	**Only for agreed professional use**	**Yes, for education use only on a school-owned device**
Use of personal email addresses in school	**NO**	**NO**
Use of school email for personal emails	**NO**	**NO**
Use of messaging apps	**Only for agreed professional and educational use**	**NO, unless it is part of a supervised Computing lesson**

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. Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school digital systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, 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, pupils or parents / carers 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.
- Pupils should be taught about online safety issues, such as 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.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Protecting (online) Personal Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

Risk assessment, including legal risk school staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or

impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process
- The school's use of social media for professional purposes will be checked regularly a senior and trained member of staff to ensure compliance with the school policies

Unsuitable and Inappropriate Activities

Online activity, such as accessing inappropriate images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities, such as cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those 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 or out outside the school when using school digital equipment or systems.

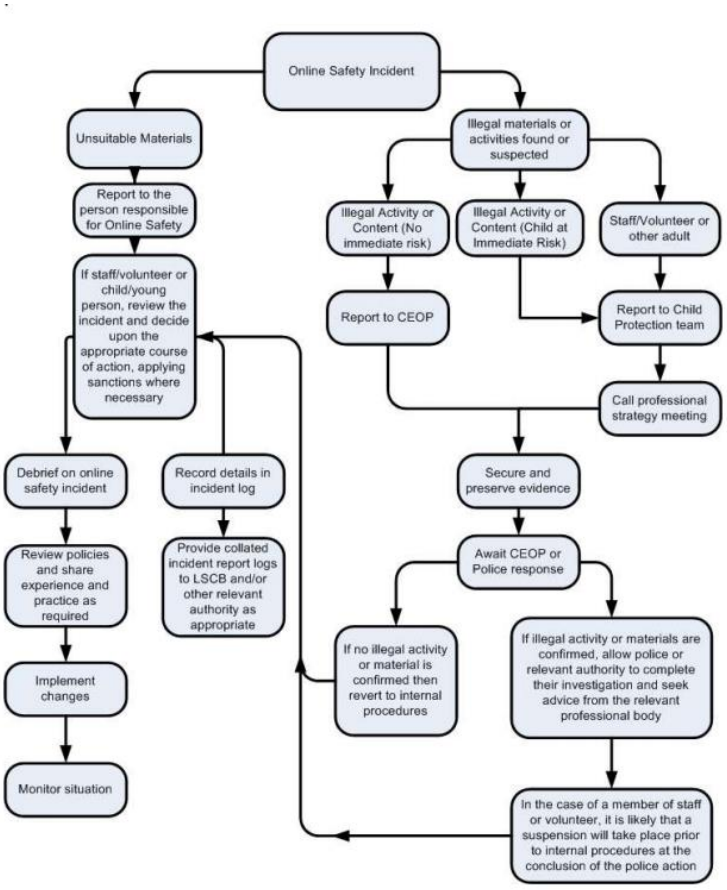
The school policy restricts usage as follows:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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
Promotion of extremism or terrorism					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					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 (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce				X	
File sharing		X			
Use of social media				X	
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube			X		

Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities. If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated device that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same device for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate online access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the device being used for investigation.

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures

- Involvement by Local Authority / Academy Trust or national / local organisation (as relevant).
- Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately.
- Other instances to report to the police would include:
- Incidents of 'grooming' behaviour o the sending of obscene materials to a child
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Promotion of terrorism or extremism
- Other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes.

School Actions and Sanctions

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 through normal behaviour / disciplinary procedures as follows:

Pupil Sanctions **X = Action(s)**	Refer to class teacher	Refer to Senior Leader	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention /
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X	X			X		X	X

Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X			X		X	X
Unauthorised / inappropriate use of social media / messaging apps / personal email	X	X		X			X	X
Unauthorised downloading or uploading of files	X	X			X			
Allowing others to access school / network by sharing username and passwords	X	X		X			X	
Attempting to access or accessing the school network, using another pupil's account	X	X		X			X	
Attempting to access or accessing the school network, using the account of a member of staff	X	X		X	X	X	X	X
Corrupting or destroying the data of other users	X	X		X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X		X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X			X	X	X	X
Using proxy sites or other means to subvert the school's filtering system		X		X			X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X	X	X	
Deliberately accessing or trying to access offensive or pornographic material	X	X		X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X		X	X	X	X	X

Staff Sanctions **X = Action(s)**	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority / HR Refer to	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email	x	x				x		
Unauthorised downloading or uploading of files	x							
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x	x			x	x		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X				X		
Deliberate actions to breach data protection or network security rules	X	X	X	X	X	X	X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	X	X	X	X	X	X	X	X
Actions which could compromise the staff member's professional standing	X	X	X			X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X	X	

Using proxy sites or other means to subvert the school's filtering system	✗	✗			✗			
Accidentally accessing offensive or pornographic material and failing to report the incident	✗	✗	✗		✗	✗	✗	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	✗	✗				✗		
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X