

Policy for: Online Safety
Author: Charlotte Gregg
***adapted from the model policy on The Key**
Date of issue: December 2023
Review date: December 2024
Signed by Chair of Governors: P.Watson



Introduction

Online Safety encompasses internet technologies and electronic communications such as mobile phones, wireless and smart technology. It highlights the need to educate the school community about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

This policy outlines the teaching, organisation and management of online safety taught and learnt at Newdigate Primary and Nursery School.

Our Aims

Newdigate Primary and Nursery School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice using technology
- Identify clear procedures to use when responding to online safety concerns

Newdigate Primary School identifies that issues classified within online safety are considerable, our approach to online safety is based on addressing the following categories of risk:

- **Content** - being exposed to illegal, inappropriate or harmful content.
- **Contact** - being subjected to harmful online interaction with other users
- **Conduct** - personal online behaviour that increases the likelihood of, or causes, harm
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

Many of these risks reflect situations in the off-line world and it is essential that this online Safety policy is used in conjunction with other school policies but not limited to:

- Safeguarding policy
- Staff code of conduct policy
- Behaviour policy

- Data Protection Policy

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Entitlement

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 ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / 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 out of school, but is linked to membership of the school.

The school will deal, as appropriate, 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 behaviour that take place out of school.

Roles and Responsibilities

The Designated Safeguarding Lead (DSL), headteacher (Geraldine Marshall – DSL) has the lead responsibility for online safety. Whilst activities of the designated safeguarding lead may be delegated to an appropriately trained deputy DSL, overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the lead DSL.

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

Governors:

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

Governors must ensure that they use their welearn email and not a personal account for any school correspondence. Mr Philip Watson as a member of the Governing Body and Online Safety Group has taken on the role of online safety Governor.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix D)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not

be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

The leadership and management team:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy and Data Protection policy, which covers acceptable use technology
- Ensure suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety
- The Headteacher is responsible 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 Subject Leader and ICT Technician.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national.

The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate
- Work alongside deputy DSL's to ensure online safety is recognised as part of the setting safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure that online safety issues are logged and dealt with appropriately in line with this policy
- Ensure any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures
- Check-up concerns during weekly DSL briefing
- Provide regular reports on online safety in school to the governing body.

Computing Lead/ICT Technician:

It is important that the ICT Technician maintains regular meetings with the Computing Subject Leader to update. The ICT LSA is Mrs A Benn and the computing subject leader is Miss C Gregg. They are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular

basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school.

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack
- the school meets the online safety technical requirements outlined in the Warwickshire Security Policy and Acceptable Usage Policy and any relevant Local Authority online safety Policy and guidance.
- Users may only access the school's networks through a properly enforced password protection and should not be shared
- The Warwickshire filtering system is working properly and reports any breaches of the filtering system to Warwickshire ICTDS.
- Keeps 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
- Within the framework of the Central Monitoring Policy provided by Warwickshire ICTDS, that she monitors the use of the schools Learning Platform, Email and other web-based services in school.

All staff and volunteers

The responsibility of all staff including contractors and agency staff, and volunteers are:

- Contribute to the development of online safety policies
- Read and adhere to the online safety policy and acceptable use policies
- Take responsibility for the security of setting systems and the data they use or have access to
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on site and offsite.
- Embed online safety education in curriculum delivery, Wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their case
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally
- Take professional responsibility for professional development in this area

Pupils (at a level that is appropriate to their individual age and ability)

- Engage in age appropriate online safety education opportunities
- Contribute to the development of online safety policies through focused online safety groups meetings which will include of the School Council members.
- Read and adhere to the acceptable use policies
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Respect the feelings and rights of others, both on and offline
- Take responsibility for keeping themselves and others safe online
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

- Know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- 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.

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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature*. The responsibility of Parents and carers are to:

- Endorse (by signature) the Student / Pupil Acceptable Use Policy
- Access the school website / learning platform / Learning platform/ pupil records in accordance with the relevant school Acceptable Use Policy.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online
- Contribute to the development of online safety policies
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Inclusion

At Newdigate Primary and Nursery School we recognise that some learners are more vulnerable online due to a range of factors. This may include, but not limited to, children in care, children with a Special Educational Needs and Disabilities (SEND) or mental health needs, children with additional language (EAL) and children experiencing trauma or loss.

- Ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.
- When implementing an appropriate online safety policy and curriculum we will seek input from specialist staff as appropriate.

Education and Engagement Approaches

The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners:

- Ensure education regarding safe and responsible use precedes internet access
- Include online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study. The teaching of online safety should follow the long and medium term plans put in place by leaders but should also be responsive to the needs of the children. These will be monitored by the Computing Lead.
- Reinforce online safety messages whenever technology or the internet is in use, as well as part of a planned programme of assemblies and pastoral activities

- 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
- Educate learners in the effective use of internet to research; including the skills of knowledge location, retrieval and evaluation
- Teach learners to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms with internet access
- Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation
- Rewarding positive use of technology (house points)
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

Extra-curricular activities

At Newdigate Primary and Nursery School we encourage children to join in extra-curricular Computing activities. We endeavour to provide as many different opportunities to engage our children in Computing, either in school or out of school hours. We provide extra-curricular opportunities through the lunch-time. Wherever possible we involve children in using Computing to pursue their interests and support work done in school. Online Safety will be given the same level of importance and consideration as formal school curricular activities.

Training

Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy.

- online safety training will be made available to staff. An audit of the online safety 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 Policies
- This Online Safety policy and its updates will be presented to and discussed by staff in staff / team meetings.
- Head teacher (Mrs G Marshall), Computing Subject Leader (Miss C Gregg) and ICT Technician (Mrs A Benn) will provide advice / guidance / training as required to individuals as required

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 Computing / online safety / health and safety / child protection. This may be offered in a number of ways:

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

Health and Safety

This needs to be read alongside our ***Health and Safety Policy, Acceptable User Policy and Computing Policy***.

- Head teacher (Mrs G Marshall), Computing Subject Leader (Miss C Gregg) and ICT Technician (Mrs A Benn) will liaise on Health and Safety issues related to computer systems.

Technical – Infrastructure/equipment, filtering and monitoring

The school uses a LA managed system and is 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 will be effective in carrying out their online safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority online Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems by ICT Technician (Mrs A Benn).

Passwords:

- All users will have clearly defined access rights to school ICT systems.
- All users at KS1 and KS2 will be provided with a username and password
- The “master / administrator” passwords for the school ICT system, used by the ICT Technician (Mrs A Benn), or other person, must also be available to the Head teacher or other nominated senior leader and kept in a secure place (e.g. school safe).
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Filtering and monitoring:

- The school is maintained and supported by the managed filtering service provided by Warwickshire LA.
- Requests from staff for sites to be removed from the filtered list will be considered by the Computing Subject Leader and ICT Technician and if the request is agreed, they will record the action and logs of such actions shall be reviewed regularly.
- School computing technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.

- An appropriate system is in place for users to report any actual / potential online safety incident to the Headteacher (or other relevant person).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed process is in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system.
- An agreed policy (AUP) is in place regarding the downloading of executable files by users. Pupils are not allowed to download files onto school system without permission.
- An agreed policy (AUP) is in place regarding the extent of personal use that users (staff /pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy (AUP) is in place that allows staff to/forbids staff from installing programmes on school workstations / portable devices. Staff are not allowed to download files onto school system without permission.
- An agreed policy (AUP) is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images – photographic, video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupil’s instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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 e.g. on future use of social networking sites.
- Staff 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 and staff should avoid any information that can directly/indirectly identify specific pupils.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data or have locked the computer if moving away temporarily from the computer.
- Transfer data using encryption and secure password protected devices.

Any supply staff must use the guest account and not use a teacher log in to access the system. This information should be given to them when arriving at school.

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 (many memory sticks / cards and other mobile devices cannot 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

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 certain internet usage, see **Appendix B**.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act

- Criminally racist material
- Other criminal conduct, activity or materials

The Headteacher (Mrs G Marshall) should be consulted and actions followed in line with the behaviour policy and advice to be given in particular when reporting the incident to the police and the preservation of evidence.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the Headteacher/DSL (Mrs G Marshall) should be informed immediately.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This included personal, social, health and economic (PHSE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behavior policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use reasonable endeavors to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots.

Newdigate Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Newdigate Primary School will treat any use of AI to bully pupils in line with our anti-bullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and educate the children about these risks.

Examining electronic devices

School staff have the specific power under the education and inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the Senior Leadership Team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out inline with:

- The DfE's latest guidance on [screening, searching and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- The school's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Appendix A:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times (HT Permission)	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school								
Use of mobile phones in lessons								
Use of mobile phones in classrooms*								
Use of mobile phones in social time, in staff-only areas e.g. staffroom								
Use of other recording devices e.g. Apple Watch**								
Taking photos on school mobile phones or other camera devices								
Use of hand held devices e.g. PDAs, PSPs								
Use of personal email addresses in school, or on school network								
Use of school email for personal emails								
Use of chat rooms / facilities (school devices)								
Use of instant messaging (school devices)								
Use of social networking sites (school devices)								
Use of blogs (school devices)								

***No mobile phones or devices with recording capabilities are permitted in Foundation Stage at all (see Foundation Stage Policies). Mobile phones must not be used in classrooms during the times which children are in school during either lessons as well as before or after clubs (8.00-4.30pm)**

****Watches being worn must have notifications turned off when they are being worn during lessons and classrooms between 8.30am-3:30pm**

Appendix B:

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated	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					☐
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					☐
	adult material that potentially breaches the Obscene Publications Act in the UK					☐
	criminally racist material in UK					☐
	pornography				☐	
	promotion of any kind of discrimination				☐	
	promotion of racial or religious hatred				☐	
	threatening behaviour, including promotion of physical violence or mental harm				☐	
	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				☐	
Using school systems to run a private business					☐	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Warwickshire LA and / or the school					☐	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					☐	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					☐	
Creating or propagating computer viruses or other harmful files					☐	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					☐	
On-line gaming (educational)				☐		
On-line gaming (non educational)					☐	
On-line gambling					☐	
On-line shopping / commerce					☐	
File sharing					☐	
Use of social networking sites					☐	
Use of video broadcasting e.g. YouTube				☐		

Students / Pupils

Actions / Sanctions

Incidents:	Refer to class teacher / Computing Coordinator	Refer to ICT Teaching Assistant	Refer to Headteacher	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 e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	☐	☐	☐	☐	☐	☐	☐	☐	☐
Unauthorised use of non-educational sites during lessons	☐	☐	☐		☐	☐	☐	☐	
Unauthorised use of mobile phone / digital camera / other handheld device	☐	☐	☐		☐	☐	☐	☐	
Unauthorised use of social networking / instant messaging / personal email	☐	☐	☐		☐	☐	☐	☐	
Unauthorised downloading or uploading of files	☐	☐			☐	☐	☐	☐	
Allowing others to access school network by sharing username and passwords	☐	☐	☐		☐	☐	☐	☐	
Attempting to access or accessing the school network, using another student's / pupil's account	☐	☐	☐		☐	☐	☐	☐	
Attempting to access or accessing the school network, using the account of a member of staff	☐	☐	☐		☐	☐	☐	☐	
Corrupting or destroying the data of other users	☐	☐	☐		☐	☐	☐	☐	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	☐	☐	☐		☐	☐	☐	☐	
Continued infringements of the above, following previous warnings or sanctions	☐	☐	☐		☐	☐	☐	☐	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	☐	☐	☐		☐	☐	☐	☐	
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	☐	☐	☐	☐	☐	☐	☐	☐	☐

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	☐	☐	☐	☐	☐	☐	☐	☐	☐
---	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------	--------------------------

Staff

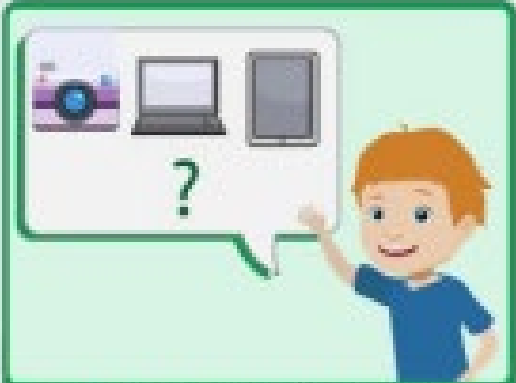
Actions / Sanctions

Incidents:	Refer to Systems Manager	Refer to Headteacher	Refer to Local Authority / HR	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).	☐	☐	☐	☐				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	☐	☐						
Unauthorised downloading or uploading of files	☐	☐						
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	☐	☐						
Careless use of personal data e.g. holding or transferring data in an insecure manner	☐	☐						
Deliberate actions to breach data protection or network security rules	☐	☐	☐					
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	☐	☐	☐					
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	☐	☐	☐			☐		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	☐	☐	☐			☐		
Actions which could compromise the staff member's professional standing	☐	☐	☐			☐		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	☐	☐	☐			☐		
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	☐	☐	☐	☐		☐		☐
Breaching copyright or licensing regulations	☐	☐	☐			☐		
Continued infringements of the above, following previous warnings or sanctions	☐	☐	☐			☐		☐



Acceptable Use Agreement

(For EYFS)



✓ I ask before I use a tablet, computer or camera.



✓ I tap or click on things I have been shown.



✓ I check if I can tap/click on things I haven't seen before.



✓ I tell a grown-up if something upsets me.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

Signed (pupil):	Date:
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	Date:

Appendix D: KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
When I use the school's ICT systems (like computers) and get onto the internet in school I will: • Ask a teacher or adult if I can do so before using them • Only use websites that a teacher or adult has told me or allowed me to use • Tell my teacher immediately if: ○ I click on a website by mistake ○ I receive messages from people I don't know ○ I find anything that may upset or harm me or my friends • Use school computers for school work only • Be kind to others and not upset or be rude to them • Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly • Only use the username and password I have been given • Try my hardest to remember my username and password • Never share my password with anyone, including my friends. • Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer • Save my work on the school network • Check with my teacher before I print anything • Log off or shut down a computer when I have finished using it I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	
Signed (pupil):	Date:
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	Date:

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will hand it into the office every morning and receive it back at the end of the school day.
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

