




Nether Hall School

ONLINE SAFETY POLICY

Policy Date:	October 2023	Policy Review Date:	October 2025
Responsible Person:	Helen Robinson		
Sarah Naylor Headteacher	Signature: 	Date:	
Adrian Keene Chair of Governors	Signature: Not Required	Date:	

Nether Hall School online-safety Policy

Introduction

In today's society, children, young people and adults interact with technologies such as mobile and smart devices, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

Online-safety covers issues relating to our pupils, other young people as well as adults and their safe use of the Internet, mobile and smart devices and other digital technologies both in and out of Nether Hall School. It includes education for all members of the school community on risks and responsibilities and is part of the safeguarding 'duty of care' which applies to everyone working with children. This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on monitoring and filtering, preventing and tackling bullying and searching, screening and confiscation of pupil property and sharing nudes and semi-nudes.

Nether Hall School provides education for pupils with Severe and Profound and Complex learning difficulties. At Nether Hall School, pupils, just like their peers in other settings, are encouraged to use digital equipment in educational, creative, empowering and fun ways. However, Nether Hall School pupils may be particularly vulnerable to online-safety risks due to their Special Educational Needs and Disabilities (SEND). For example:

- Some pupils may not understand terminology used due to their severe or profound learning difficulties or their severe communication difficulties.
- Some pupils with SEND may be vulnerable to being bullied through the use of electronic communication, or not recognise that they are being bullied.
- Some pupils may unwittingly share information, pictures or videos with others thereby putting themselves at risk.
- Some pupils may be particularly vulnerable to grooming through online gaming and other online activities.
- In addition, some pupils may not appreciate how their own online behaviour may be seen by others as a problem, threat or even criminal.

Aims

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 protects and educates the whole school community in its use of technology, including mobile and smart technology
- Establish clear processes to identify, intervene and escalate an incident, where appropriate
-

The 4 key categories of risk

Our approach to pupil online safety is based on addressing the following categories of risk:

- Content – Pupils being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, radicalisation and extremism
- Contact – Pupils being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults with the intention to groom or exploit
- Conduct – Pupil online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

- Commerce – risks to pupils such as online gambling, inappropriate advertising, in app purchasing, phishing and/or financial scams

Online-safety Roles and responsibilities

The governing body has overall responsibility for monitoring this policy and holding the Head Teacher to account for its implementation.

The Head Teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. The Head Teacher ensures that filtering and monitoring of school devices and networks is in place. The Head Teacher designates a deputy DSL as the designated online-safety safeguarding lead. The online-safety safeguarding lead takes principal responsibility for online safety in school, in particular:

- Supporting the Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Ensuring appropriate filtering and monitoring approaches are in place which are suitable for the local context and use of technology. The leadership team and relevant staff should have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.
- Working with the Head Teacher, Business Manager, ICT Technicians and other staff, as necessary, to address any online-safety issues, incidents, concerns and compliancy
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents and any incidents of cyber-bullying are logged and dealt with appropriately in line with this policy
- Updating and providing staff training on online safety including an ‘understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring’.
- Ensuring Online safety approaches are regularly reviewed and updated as required.
- Liaising with other agencies and/or external services as necessary.

Lead DSL: Sarah Naylor - Head Teacher

Online-safety Deputies: DSL: Helen Robinson – Assistant Headteacher

Management of assets

Details of all school-owned hardware and software are recorded in an inventory.

Redundant IT equipment is disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. Where possible Nether Hall school will destroy all personal data before disposal of equipment.

Teaching and learning with Electronic Communication Devices

Pupils will be taught to use a range of digital technologies to access the Internet, games machines and mobile technologies within a personal safety context. Use of the school’s internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual’s role. All users are digitally monitored and filtered using a subscription monitoring service.

Internet access

The school’s Internet access is designed to enhance and extend education.

- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils’ age and ability.
- Throughout the curriculum, Nether Hall School pupils will be taught to ‘Stop and Tell’ if content upsets, frightens or makes them feel anxious. Visual reminders will be provided as prompts for what to do if they have concerns when using digital technologies. Pupils will be taught to use technology safely, respectfully and responsibly.
- Pupils will be provided with age-appropriate tools to search and access Internet content.

- The school will maintain a current record of all staff, governors, volunteers and pupils who are granted access to the school's electronic communications.
- All staff, volunteers and governors will read and sign the 'Acceptable Use Policy' before using any school ICT digital devices. There will be regular online safety updates for all staff.
- Parents will read and sign the 'Pupil Acceptable Use Policy' annually and be informed that pupils will be provided with Internet access appropriate to their age and ability.
- Primary and Asteroid Pathway pupils' access to the Internet will be by adult demonstration with directly supervised access to filtered online materials.
- Older and more able pupils may use age-appropriate search engines and online tools, with supervision. Online activities will be teacher-directed where necessary.
- The school will take all reasonable precautions to ensure that users access only appropriate materials. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer or digital device. The School Governors, School and Leicester City Council cannot accept liability for any materials accessed, or any consequences resulting from Internet use by Nether Hall pupils.

Digital communication - Email /SMS (Direct or via Arbor)

Digital communication is an essential means of communication for staff and can enrich pupils' learning. Selected pupils may be provided with individual email accounts for school purposes, where appropriate. Pupils may be taught how to create and send text messages.

- Staff must ensure any digital communications with pupils and parents / carers (email / text/ social media and voice) must be professional in tone and content and be via Nether Hall School systems.
- Staff will not forward or share emails, other than in a professional capacity, with outside agencies.
- Any sensitive documents will be password protected if anycomms or similar secure transfer is unavailable.
- Pupils, using individual email accounts, will be taught to immediately tell a member of staff if they receive an email that concerns, worries or upsets them. The school reserves the right to read all email sent to and by our pupils.
- Pupils will be supported to understand that they must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without supervision of school staff.

Publishing Electronically

Publishing images on the school website or on school social media pages can enhance experiences for pupils and allow staff to share achievements quickly with parents. The material included on the school's website / social media platforms will be limited to pupils with parent /carer permissions and uploaded with very general labels. Images or video of individual children will only be used in exceptional circumstances to promote individual achievements. At no time will personal email / postal addresses, telephone / fax numbers be shown.

- Permission from parents or carers must be obtained before images/videos of pupils are electronically published.
- Large images will be avoided or locked to restrict others from reusing the image.
- Pupils' full names will not be used anywhere in electronic communications particularly in association with photographs and the school.

Social networking, social media and personal publishing

Social media and personal publishing tools include: blogs, wikis, social networking, social media video apps, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

As appropriate (determined by the age and ability of pupils) pupils will be taught to think about the ease of uploading personal information, videos and images and the associated dangers as well as the difficulty of removing an inappropriate image or information once published.

All staff are made aware of the potential risks of using social networking sites or personal publishing either professionally with pupils or personally. They are made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing or sharing unsuitable material, in any format, may affect their professional status.

- The school will control access to social media and social networking sites through filtering.
- Staff wishing to use social media tools / apps with pupils as part of the curriculum will risk assess the sites / apps before use and check the sites terms and conditions to ensure the site is appropriate for use with our pupils.
- Staff will ensure that only school email and web addresses are employed.
- Staff will ensure parental / carer permission is granted before publishing pupils' images on any platform.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Code of Conduct Policy. (Section 5. Staff/pupil relationships, Section 7. Communication and social media, Section 8. Acceptable use of technology and Section 13. Conduct outside of work)
- Where appropriate, pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples include: pupils real name, address, mobile or landline phone numbers and school attended.
- Within the curriculum and specifically within the Problem Solving and Thinking Skills (PSTS) computing curriculum; pupils will be taught about security and privacy online and will be supported, at school, to set passwords, deny access to unknown individuals and to block unwanted communications.

Web filtering/ Monitoring (Netsweeper)

There are two levels of access provided by the schools filtering service. For educational purposes staff will have access to a number of websites that pupils may not.

By default, the school's internet filtering software blocks the following content for both staff and pupils:

- Adult content containing sexually explicit images, video or text
- Violent content containing graphically violent images, video or text
- Hate Material content which promotes violence or attack on individuals or institutions on the basis of religious, racial or gender grounds
- Illegal drug taking and the promotion of illegal drug use
- Gambling content
- Grey Filtering - this covers websites that although may not be deemed inappropriate are not necessarily educational. These include gaming websites, social networking sites and others agreed by the senior leadership team.

Any user at school may not access, distribute or place online material that:

- is illegal in the UK
- is offensive, obscene, encourages or facilitates illegal activities
- is in breach of copyright owners' statutory rights
- could be used to harass or intimidate another person, when using email, messaging or chat.

Access profiles must be appropriate for all members of the school community and designated accordingly. Older pupils, as part of a supervised project, might need to access specific adult materials; for instance, a course might include sexual relationships. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use will be recognised and allowed. Where a member of staff wishes to access a website, that is currently blocked by the filters, they should request approval from their phase leader or the Head Teacher.

Internet safety rules are provided to be displayed in all teaching areas, and pupils should be educated about the risks online. It is recognised by Nether Hall School that filtering is not 100% effective. Staff are educated about risks online, however, occasionally mistakes happen and inappropriate content may be accessed. It is

therefore important that pupils are supervised. The Online Safety Incident Log must be used to report breaches of filtering or inappropriate content being accessed. Any breaches will be shared with the Lead DSL, entered on CPOMs and actioned accordingly. Any material that the school believes is illegal must be reported to the appropriate agencies.

- Teachers should always attempt to evaluate any websites/search engines before using them with their pupils; this includes websites shown in class as well as websites accessed directly by the pupils. Often this will mean checking the websites, search results etc just before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity.
- It is recognised that many of our pupils will be very 'quick to click' and may have navigated to undesirable materials accidentally; often incidents will be reported with no further action taken with the pupil. Where appropriate, pupils will be advised individually.

The school will ensure: -

- Pupils are taught when using the Internet to 'Stop and Tell' if concerned about any content they see or read. Supervised use of online materials will ensure pupils are supported if they are concerned by any accessed content.
- Where appropriate to the individual pupil, they are taught about the risks online.
- Filtering and monitoring systems installed across the network and digital devices (at an appropriate level for the pupils) are updated on a regular basis and reports provided to the Head teacher and DSLs.
- ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly including laptops and other mobile devices.
- Security of the school's ICT systems is checked and monitored on a monthly basis by the school's ICT Technician.
- Access is blocked to potentially dangerous sites and, where possible, prevents the downloading of potentially dangerous files.
- Volunteers, visitors and contractors cannot access the school's secure ICT systems, visitors have limited access to some software. Internet usage by volunteers, visitors and contractors is filtered and monitored.
- Online safety incidents are logged and dealt with appropriately in line with this policy.
- Incidents of cyber-bullying, sexting etc. are dealt with appropriately, in line with the school behaviour policy.

All staff will: -

- Ensure they understand and Implement this policy consistently.
- Never share passwords with others or allow others to login in their name.
- Never allow pupils to use their staff login.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet as outlined in the Acceptable Use Policy.
- Ensure that pupils do not access the internet without parental permission.
- Ensure pupils are supervised when accessing the internet and when using digital technologies.
- Ensure pupils are guided to sites that are checked as suitable for their use in lessons where internet use is planned.
- Log any incidences of unsuitable materials being accessed by pupils on the appropriate form with DSLs, the ICT technician and via CPOMs.
- Ensure that any digital communications with pupils and parents / carers (text / image/ voice) are on a professional level.
- Ensure that any incidents of cyber-bullying etc are dealt with appropriately in line with the school behaviour policy.
- Supervise any volunteers or contractors using the schools Internet in the presence of pupils.

Video conferencing

Videoconferencing enables users to see and hear each other between different locations. It is a powerful teaching tool allowing pupils to see and access others in locations outside of school. Video conferencing may be used to support home learning, for parents /carers and pupils to attend meetings and to join in with school activities such as assemblies and performances.

To use video conferencing safely staff will ensure: -

- Parents / carers consent has been obtained prior to pupils taking part in video conferences outside of the school network.
- All video conferencing equipment in the classroom is switched off when not in use and not set to auto answer.
- External IP addresses are not made available to other sites.
- Video conferencing contact information is not accessible from the school website.
- Unique logon and password details are issued to members of staff and kept secure.

In addition; staff, pupils and parents / carers using video or audio communication must:

- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable ‘public’ living area within the home with an appropriate background – ‘private’ living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Always remain aware that they are visible or can be heard.

If any safeguarding concerns arise through the use of video or audio-conferencing staff will report any safeguarding concerns to the DSL immediately and record on CPOMs system.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, and can access school websites and home / school activities where provided. The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, monitoring and filtering systems, on devices not owned by the school.

When learning online or via video conferencing the school will maintain contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. activities / sites they have been asked to use and how school they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

Emerging technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken for each new technology for effective and safe practice with pupils to be developed. The risk assessment will be referenced in teacher planning.

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers, such as, a pupil using a phone to video a teacher’s reaction in a difficult situation.

Therefore, the school will ensure: -

- Emerging technologies will be examined for educational benefit and an assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices, both on and off site, through the personal and social development (PSD) curriculum and the computing element of the problem solving and thinking skills curriculum.

Cyberbullying (including sexting)

Cyber-bullying takes place online, such as through social media sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. Pupils will be taught, where appropriate, how to recognise the signs of cyberbullying within the curriculum and when using digital technologies.

The school will ensure: -

- Cyberbullying (along with all other forms of bullying) of any member of the school community is not tolerated. Full details are set out in the school's Anti Bullying policy.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school, are recorded.
- There are clear procedures in place to investigate incidents or allegations of cyberbullying, allowing for the intellectual abilities of the pupil concerned.
- Staff and parents / carers are advised to keep a record of the cyberbullying as evidence.

Mobile and Smart Devices

Mobile phones and other personal digital devices such as wearable technology, Games Consoles, Tablets, and MP3 Players etc. are considered to be an everyday item in today's society and even pupils in early years may own and use personal devices online regularly. However, their use in school could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff. Where appropriate pupils may bring a mobile phone to school. However, an acceptable use agreement must be signed by both the parent and the pupil before it can be used in school. Parents sign agreement to pupil phone content (created within school) being monitored and if necessarily deleted by school staff.

Staff, volunteers, parents and pupils, where appropriate, are informed that: -

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with using discipline procedures.
- Schools digital devices, mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms and toilets. No personal staff devices are allowed for recording within any swimming activity.
- Mobile phones and wearable technologies will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity. Members of staff must have approval from the Senior Leadership Team to allow pupil use of mobile phones or personal devices as part of an educational activity. E.g. fitness tracker.
- Teaching staff ensure pupils are taught, where appropriate, to use devices with regard to personal safety and the feelings of others. Pupils are taught to gain consent before recording / photographing others.
- School staff may confiscate a phone or other personal device if they believe it is being used inappropriately. 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 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. Staff, if they believe an electronic device may contain sexual images of a child, they must not view the images. If they believe an electronic device may contain evidence of an offence, such as child pornography or an extreme pornographic image, they must not delete anything. Devices must be given to a DSL immediately, the device will be passed to the police etc

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

- Electronic devices of all kinds, including mobile phones and wearable technology, that are brought in to school by pupils are the responsibility of the pupil. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Pupils Use of Personal Devices:

We recognise a small number of pupils may wish to bring mobile devices into school. Where this is the case, arrangements will be agreed with the parents /carers and an acceptable use form will be completed. The wearing of digital devices such as smart watches is discouraged due to the cost of the items, the likelihood of them becoming lost or damaged and the difficulties in monitoring potential recordings and access to the internet. All mobile devices brought to school are done so at the pupil's own risk, they are responsible for its safe-keeping and the school cannot be held responsible for any loss or damage.

Pupils are not permitted to use personal mobile devices and wearable devices such as smart watches during:

- Lessons, break times and lunchtime unless supervised and agreed with classroom staff
- Clubs before or after school, or any other activities organised by the school unless supervised and agreed with staff
- To take photographs, videos or audio recordings of pupils or staff. *{In exceptional circumstances, agreed in advance by the Head Teacher, photography may be approved if the parents/ carers of other pupils agree and staff agree. For example, at the leaver's assembly, a birthday or special occasion.}*
- To connect to the internet either via Wi-Fi or mobile connectivity such as 3, 4 or 5G.

Pupil, parent / carer responsibility:

- Understand that any pupil breaching the school policy will result in the phone or device being confiscated and held in a secure place in the school office until released to parents / carers. We reserve the right to delete data from confiscated device or to ensure the parent / carer does so.
- Recognise the potential dangers associated with unmonitored access to the internet provided by internet access technology now found in many mobile devices.
- Refrain from contacting their child whilst in school or attending school activities. Urgent messages from parents/ carers should be passed through the school office.
- Understand pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Mobile phones are permitted on school residential activities, although they remain the responsibility of the user. Mobile phone use is limited to times supervised and agreed with staff. We discourage pupils from contacting home while attending residential as it may lead to anxiety. Instead, parents / carers are encouraged to contact accompanying staff on a number provided.

Staff Use of Personal Devices

- Staff should refrain from using their own personal phones or devices for contacting pupil's families within or outside of the setting in a professional capacity.
- Staff may be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile phones, wearable technology and other devices will be switched off or switched to 'silent' mode, during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- Staff should not use personal devices such as mobile phones, smart watches or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Staff should not connect personal devices to the school Wi-Fi.
- Wearable technologies such as smart watches are permitted to be worn by staff but to be used as only a watch around the pupils.

Staff using school owned and provided devices and software/apps outside school

- Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.
- Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.
- Systems accessed on personal devices such as e-mail, CPOMS and Evidence for Learning must be logged out of at the completion of access.
- Any USB devices containing data relating to the school must be encrypted.
- If staff have any concerns over the security of their device, they must seek advice from the ICT technician.
- Work devices must be used solely for work activities. They must be solely used by people in the employ of Nether Hall School.

Responding to any incidents of concern

- It is recognised that many of our pupils will be very 'quick to click' and may have navigated to undesirable materials accidentally. They may also, for example, send an obscene word to a friend or distribute an inappropriate image. An internal investigation would be appropriate in most of these circumstances. We are aware that a number of pupils are over 18. External advice will be sought in these incidences.
- Incidents of concern will be logged on CPOMS including an online safety incident log.
- The school will inform parents/carers of any incidents of concern, as and when required.
- Complaints about Internet misuse will be dealt with under the school's complaints procedure.
- All staff will be informed about the procedure for reporting online-safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- All online-safety complaints and incidents will be recorded by the school, including any actions taken.
- The Lead DSL will monitor all reported incidents and actions taken in the school online-safety incident log.
- The DSLs will be informed of any online-safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage online-safety incidents in accordance with the school behaviour policy where appropriate.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
- online-safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the LA Safeguarding Team or online-safety officer and escalate the concern to the Police and Child Exploitation and Online Protection (CEOP).
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

School community awareness

- All users will be informed that network and Internet use is monitored.
- Annual online-safety training will be established across the school to raise the awareness and importance of safe and responsible internet and mobile device use for staff supporting pupils.
- Pupils, where appropriate, will be taught and demonstrated responsible and safe use of the internet and other electronic devices across the curriculum.

- An online-safety module will be included in the PSD and computing programmes for more able pupils (Meteors and where appropriate Comets) covering both safe school and home use of electronic and online devices.
- All members of staff are regularly reminded that their online conduct out of school could have an impact on their role and reputation within school. Civil, disciplinary or legal action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Home use

Online use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home.

- A partnership approach to online-safety at home and at school with parents will be encouraged. This may include offering parent workshops with demonstrations and suggestions for safe home Internet use, or highlighting online-safety at other attended events e.g. sports days.
- Information and guidance for parents online-safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.

Links with other policies / documents

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- **Teaching online safety in schools**
- **Meeting digital and technology standards in schools and colleges**
- **Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff**
- **Relationships and sex education**
- **Sharing nudes and semi-nudes: advice for education settings working with children and young people**
- **Searching, screening and confiscation**

It also refers to the DfE's guidance on protecting children from radicalisation.

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Anti Bullying
- Behaviour policy
- Staff code of conduct policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Staff Acceptable Use policy
- Pupil Acceptable Use policies
- Mobile phone Acceptable use – pupil agreement