

Endon Hall Primary & Nursery School

'Inspire today to achieve tomorrow'



Online Safety Policy

Policy in place: Sept 2016

Reviewed annually/Last review: July 2025

Review date: July 2026

	Member of staff responsible	Governor	Senior member of staff
Online Safety	Miss A Coleman/ Miss J Hughes –	Mrs Soboljew	Miss V Lewis

Contents:

1. Introduction
2. Aims
3. Use of the internet
4. School website
5. Roles and responsibilities
6. Technical – infrastructure / equipment, filtering and monitoring
7. Online safety education and training
8. Curriculum
9. Use of Digital and Video images - Photographic, Video (see policy for use of photos and images)
10. Cyber bullying
11. Cyber crime
12. Communications
13. Data protection
14. Data security
15. Unsuitable / inappropriate / illegal activities
16. Responding to incidents of misuse
17. Social networking and personal publishing
18. Use of Smart technology and devices
19. Online hoaxes and harmful online challenges
20. Grooming and exploitation
21. Mental Health
22. Generative artificial intelligence (AI)
23. Educating Parents
24. Appendix

1. Introduction

At Endon Hall Primary & Nursery School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst Endon Hall Primary & Nursery School recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material e.g. pornography, fake news, and racist or radical and extremist views.
- **Contact:** Being subjected to harmful online interaction with other users e.g. commercial advertising and/or adults posing as children or young adults.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm e.g. sending and receiving explicit messages, and/or cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Legal framework

This policy has due regard to the following legislation, including, but not limited to:

- The Human Rights Act 1998
- The General Data Protection Regulation 2016
- The Regulation of Investigatory Powers Act 2000
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspections Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- DfE (2021) 'Harmful online challenges and online hoaxes'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2023) 'Generative artificial intelligence in education'
- DfE (2024) 'Filtering and monitoring standards for schools and colleges'

This policy also has regard to the following statutory guidance:

- DfE (2024) 'Keeping children safe in education 2024'

2. Aims

- To actively provide and promote opportunities for developing pupils' skills to develop safe online behaviour.
- To ensure that staff are able to identify and respond to all potential forms of online safety incidents.
- To ensure that children and young people are aware of how and to whom online safety incidents should be reported and understand that all online safety concerns will be dealt with sensitively and effectively.
- To ensure that parents/carers are aware of online safety issues and know whom to contact if they are worried about online safety issues.

3. Use of the internet

The school understands that using the internet is not only a skill that children need to learn but an important tool in enhancing teaching and learning.

Internet use is embedded in the statutory curriculum and is therefore an entitlement for all children. However, there are a number of controls required in order to minimise harmful risks.

When accessing the internet, individuals are vulnerable to a number of risks which may be physically and emotionally harmful.

These risks include the following:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge
- Being subject to persuasive behaviour

4. School Website

The contact details on the website show the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified without parental consent.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Permission may be requested from pupils and parents or carers, before their work will be considered for publication.

5. Roles and Responsibilities

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

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Pupil & Curriculum Committee and/or Computing link governor receiving regular information about online safety incidents and monitoring reports. The Online Safety Governor representative is Mrs Soboljew.

The role of the Online Safety Governor will include:

- Termly meetings with the Online Safety Lead
- Monitoring/awareness of Online Safety incident logs
- Reporting to relevant Governors' committee
- Ensuring that relevant school policies have an effective approach to planning for, and/or responding to, online challenges and hoaxes.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.

Headteacher and Senior Leaders

- 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 Online Safety Co-ordinator.
- The Headteacher/Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, where relevant.
- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those 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. Monitoring may be carried out via methods such as

planning and work scrutinies, assessment and coverage overviews and pupil conversations. Outcomes including areas for development will be shared with staff and addressed through the School Improvement Plan.

- The Senior Leadership Team will receive regular feedback from the Online Safety Lead.
- The Headteacher and Assistant Headteacher (as designated child protection persons) will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see Section 14).
- The Headteacher is responsible for ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- The Headteacher is responsible for ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.

Online Safety Lead

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Liaises with school IT technical staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meets termly with the Online Safety Governor to discuss current issues/review logs.
- Attends relevant Governors meetings.
- Reports regularly to the Senior Leadership Team
- Gives (at least) termly updates regarding Online Safety risks
- Conducts a yearly survey to analyse the children's use and risks when online

All online safety incidents will be reported immediately to the Headteacher/Deputy/Assistant Headteacher to decide the most appropriate way of dealing with them and whether the incidents are child protection issues, in which case they will be dealt with in accordance with the school's Child Protection & Safeguarding Policy. This applies to online safety incidents both in and out of school, where incidents out of school are brought to the attention of the school and/or are impacting on children in school.

Technical staff

The Computing Lead is responsible for ensuring:

- That the school's IT infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets the online safety technical requirements outlined in the Staffordshire Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance.
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- That he/she 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.
- That the use of the network/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Lead/Headteacher/Deputy Headteacher/Assistant Headteacher for investigation/action/sanction.
- That monitoring software/systems are implemented and updated as agreed in school policies.

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 school Staff Acceptable Use Policy/Agreement (AUP).
- They report any suspected misuse or problem to the Online Safety Lead/Headteacher/Deputy Headteacher/Assistant Headteacher for investigation/action/sanction.
- Digital communications with pupils (email/voice) 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 school activities.
- Pupils understand and follow the school Online Safety and Acceptable Use Policy.

- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor IT activity in lessons, extra-curricular and extended school activities.
- They are aware of online safety issues related to the use of mobile phones, tablets, cameras and hand held devices and that they monitor their use and implement current school 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.

The Designated Safeguarding Lead (DSL) will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so that they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff regarding online safety matters e.g. the SENDCo and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by children and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- Understanding the purpose of record keeping.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the Governing Board about online safety on a termly basis.
- Working with the Headteacher and ICT technicians to conduct termly light-touch reviews of this policy.
- Working with the Headteacher and Governing Board to update this policy on an annual basis.

Pupils

- Are responsible for using the school IT systems in accordance with the Pupil Acceptable Use Policy which is provided at the start of their time at the school and again when entering KS2. Parents/carers may sign on behalf of the pupils.
- Will be taught to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones, tablets, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

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 IT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local online safety campaigns/literature. Parents and carers will be responsible for:

- Endorsing (by child/parent signature) the Pupil Acceptable Use Policy
- Accessing the school website in accordance with the relevant school Acceptable Use Policy
- Following the Parent/Carer Code of Conduct (including Social Networking) Policy
- Following the Remote Learning, Communication and Acceptable Use Policy
- Understanding the importance of their child adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their child's actions out of school, if related to their membership of the school.

6. Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school 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.

The Governing Board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The Governing Board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The Designated Safeguarding Lead (DSL) will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

- School IT 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 IT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school IT systems. Details of the access rights available to groups of users will be recorded by the Computing Lead and will be reviewed annually.
- The "master/administrator" passwords for the school IT system, used by the IT technician (or other person) must also be available to the Headteacher (on request). The school will never allow one user to have sole administrator access.
- Users are responsible for the security of their username and password. They 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, although when working in pairs in the IT suite it will be necessary for pupils to share their partner's log-on.
- The school maintains and supports the managed filtering service provided by the Local Authority.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to Entrust.
- Requests from staff for sites to be removed from the filtered list will be considered by the Computing Lead and Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.
- School IT technical staff regularly monitor and record the activity of users on the school IT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users' activity.
- An appropriate system is in place (see Appendix 1) to be given to Online safety co-ordinator immediately after incident) for users to report any actual/potential online safety incident to the Online Safety Lead.
- Appropriate security measures are in place (PCE) 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 policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system – guest log-ons are available.
- An agreed policy is in place regarding the use of removable media. No memory sticks are permitted to be used unless they have been encrypted by the school's IT technician. Users must utilise the schools' Remote Desktop Server (RDS) as their default method for accessing any work related documents away from the school premises. Only if they are unable to access the RDS can they utilise their encrypted memory stick. Where possible, the RDS should be accessed from a device which is owned and provided by the school.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal or sensitive data cannot be sent over the internet (unless password protected) or taken off the school site unless safely encrypted or otherwise secured (see School Personal Data Policy).
- When documents sent electronically are password protected the recipient will be asked to reply to the e-mail to request the password. This enables staff to check the validity of the recipient before the password is released.
- If accessing work e-mails via their smart phones, staff will utilise the Office 365 app or a link on the home screen to the Office 365 login page. Notifications will be switched off. The smart phone will require a passcode to unlock it. The app/home screen link will require a password to access it. Staff will sign out after each use.

7. Online Safety Education and Training

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 education will be provided at Endon Hall Primary & Nursery School in the following ways:

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RSHE - through our 'Pants' unit of work (taught annually from Nursery – Year 2) and, in KS2, through the 'Online Relationships' unit/s of work
- Computing

Online safety teaching is always appropriate to pupils' ages and developmental stages.

- Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:
 - How to evaluate what they see online
 - How to recognise techniques used for persuasion
 - Acceptable and unacceptable online behaviour
 - How to identify online risks
 - How and when to seek support
 - How to identify when something is deliberately deceitful or harmful
 - How to recognise when something they are being asked to do puts them at risk and/or is age-inappropriate
 - Knowledge and behaviours that are covered in the Government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix A of this policy.

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff e.g. the SENDCo and designated teacher for Looked After Children (LAC), will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms e.g. pupils with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection & Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection & Safeguarding Policy.

Planned sessions will include (Appendix 4):

- Throughout the TeachComputing lessons, pupils will be taught how to use technology safely and respectfully, keeping personal information private and how to identify where to go when they need help and support, have concerns about content, or how to contact on the internet or other online technologies
- Key online safety messages will be reinforced as part of a planned programme of assemblies and learning activities
- Key whole school celebrations on a yearly basis (Safer Internet Day)
- Pupils will 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 will be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside school
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of IT systems/internet will be posted in all rooms
- Staff will act as good role models in their use of IT, the internet and mobile devices

Parents and Carers

Many parents/carers may 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 their child/ren's online experiences.

Parents/carers often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters/newsletters
- The school website
- The school Facebook page
- Parents evenings/meetings
- Other events

Staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Governors

Governors will take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in IT/online safety/health and safety/child protection. 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 and/or parents/carers.

8. Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of IT across the curriculum.

- In lessons where internet use is pre-planned, pupils will be guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet e.g. using search engines, staff will be vigilant in monitoring the content of the websites the pupils visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation,

staff can request that the Computing Co-ordinator/Headteacher can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. Requests for website release should be made on an appropriate request proforma (see Appendix 2).

- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet and to be aware of the potential consequences of plagiarism.

9. Use of Digital and Video images - Photographic, Video (see policy for use of photos and images)

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 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. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet 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 will 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 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. Pupils and members of staff may use digital cameras to record evidence of educational activities in lessons and during school related off site activities. These images may then be used in presentations in subsequent lessons.
- Images may also be used to celebrate success through their publication in newsletters, editions of the school's newspaper, on the school website, on the school Facebook page and occasionally in the public media.
- Care will 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (consent form signed by parents or carers at the start of every year).

10. Cyber Bullying

Opportunities for pupils to bully or to be bullied via technology, such as e-mail, texts or a wide range of social media sites are becoming more frequent nationally. As such, teaching pupils about appropriate behaviours when using technology provides a vital grounding for future use. Whilst not wanting to provoke unrecognised opportunities in pupils, consideration must be given to suitable teaching and procedures to address any issues of cyber-bullying.

- The school's Anti-Bullying Policy will address Cyber-bullying (see Anti-Bullying Policy).
- Pupils, parents, staff and governors will all be made aware of the consequences of cyber-bullying. Young people and their parents will be made aware of pupils' rights and responsibilities in their use of new technologies and what the sanctions are for misuse.
- Parents/carers will be provided with an opportunity to find out more about cyber-bullying through information and/or sessions for parents.
- The school will take all reasonable precautions to ensure against cyber-bullying whilst pupils are in its care. However, due to the global and connected nature of new technologies, it is not possible to guarantee that inappropriate use via a school computer will not occur. Neither the school, nor Staffordshire County Council can accept liability for inappropriate use, or any consequences resulting outside of school.
- As part of the Online Safety and RSHE curriculum, planned sessions regarding Online Relationships will be delivered on a yearly basis in Computing sessions.

The school will proactively engage with pupils in preventing cyber-bullying by:

- Understanding and talking about cyber-bullying e.g. inappropriate use of e-mail, text messages etc;
- Keeping existing policies and practices up to date with new technologies;

- Ensuring easy and comfortable procedures for reporting;
- Promoting the positive use of technology;
- Evaluating the impact of prevention activities.

Records of any incidents of cyber-bullying will be kept and used to help to monitor the effectiveness of the school's prevention activities.

11. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the Designated Safeguarding Lead (DSL) will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and Headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

In addition, the school will implement a cyber awareness plan for pupils and staff to ensure that they understand the basics of cyber security and protecting themselves from cyber crime. This will be done through:

- Delivery of our online safety curriculum
- Understanding of and consenting to the AUP
- Staff online Cyber Security training

The school will implement its cyber security strategy in line with the DfE's 'Cyber security standards for schools and colleges' and the Cyber Security Policy.

12. Communications

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:

Please tick ✓	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies								
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time		✓						✓

Taking photos on 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				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓				✓
Use of blogs		✓					✓	

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. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers (email, chat, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They will also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information will not be posted on the school website and only official email addresses should be used to identify members of staff.

13. Data Protection

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2016 which states that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

14. Data security

- Confidential paper records will be kept in a filing cabinet, cupboard, drawer or safe, all securely locked and with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Digital data is encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up.
- Where data is saved on removable storage or a portable device, the device will be encrypted and/or kept in a locked filing cabinet, drawer or safe when not in use.
- An agreed policy is in place regarding the use of removable media. No memory sticks are permitted to be used unless they have been encrypted by the school's IT technician. Users must utilise the schools' Remote Desktop Server (RDS) as their default method for accessing any work related documents away from the school premises. Only if they are unable to access the RDS can they utilise their encrypted memory stick. The RDS should be accessed from a device which is owned and provided by the school.
- Staff will not use their personal laptops or computers for school purposes.
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts (every 60 days) users to change their password.
- Emails containing personal or sensitive information are password-protected if there are unsecure servers between the sender and the recipient.
- Circular emails to groups of people, including parents, must be sent blind carbon copy (bcc), so that email addresses are not disclosed to other recipients. This is with the exception of internal group e-mails e.g. @endonhall.staffs.sch.uk
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.
- Before sharing data, all staff members will ensure:
 - They are allowed to share it
 - That adequate security is in place to protect it
 - Who will receive the data has been outlined in a privacy notice
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.
- The physical security of the school's buildings and storage systems, and access to them, is reviewed on a **termly** basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
- Endon Hall Primary & Nursery School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- The Headteacher is responsible for continuity and recovery measures in place to ensure the security of protected data.

15. Unsuitable/inappropriate/illegal activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other IT systems. Other activities e.g. 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 avoids unnecessarily criminalising pupils e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy. Advice will be sought from the Safeguarding Advice Team/LADO wherever necessary.

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 as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	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 the 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				✓	
Online gaming (educational)			✓		
Online gaming (non-educational)				✓	
Online gambling				✓	
Online shopping / commerce		✓			
File sharing			✓		
Use of social networking sites				✓	
Use of video broadcasting e.g. YouTube		✓			

16. Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of IT, 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:

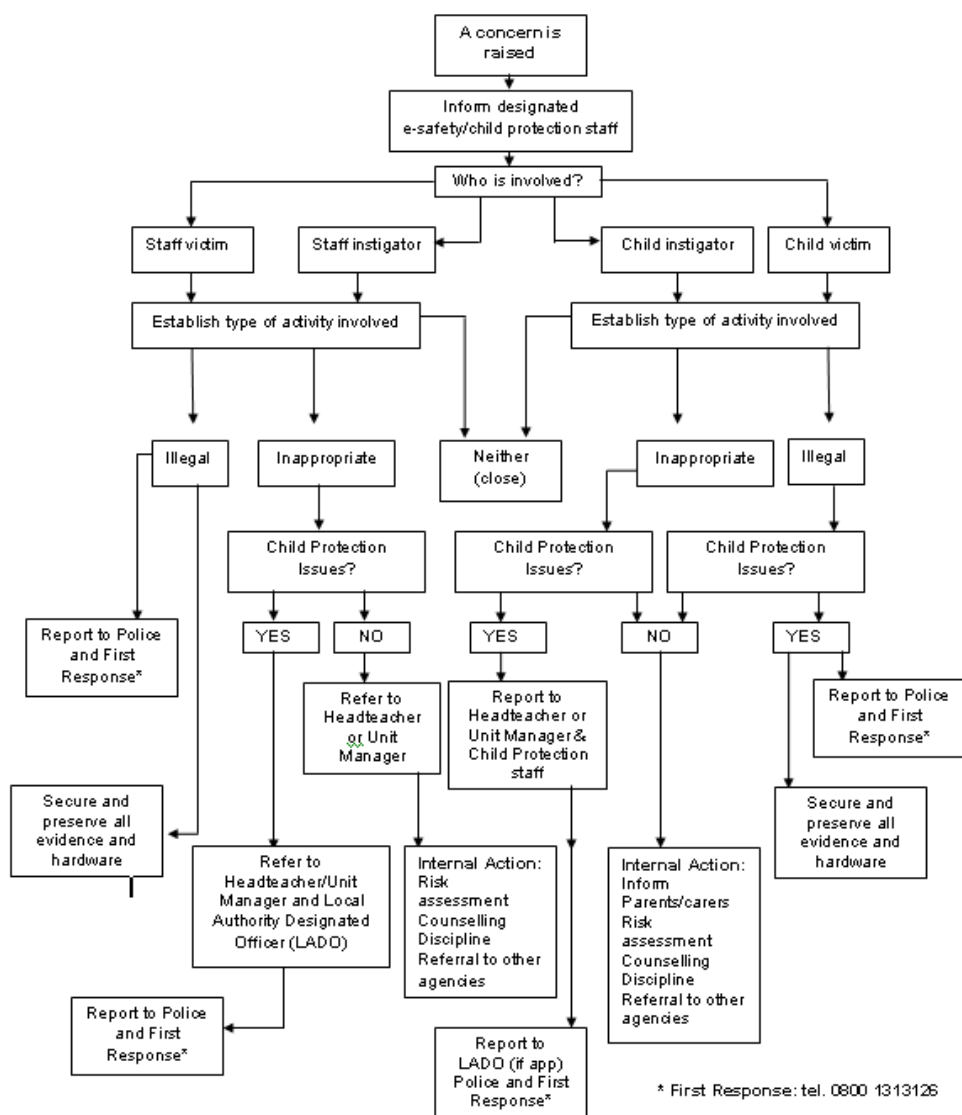
If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The flow chart from the Staffordshire Safeguarding Children's board is below and

[http://www.staffsscb.org.uk/Professionals/Key-Safeguarding/online safety/online safety-Toolkit/Incident-Response/Incident-Response.aspx](http://www.staffsscb.org.uk/Professionals/Key-Safeguarding/online%20safety/online%20safety-Toolkit/Incident-Response/Incident-Response.aspx) should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

Staffordshire Local Safeguarding Children Board



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 an event contact will be made with the Staffordshire Safeguarding Children's Board.

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.

Child-on-Child Sexual Abuse and Harassment

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking “sides”, often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection & Safeguarding Policy.

17. Social networking and personal publishing

Use of social media on behalf of Endon Hall Primary & Nursery School will be conducted following the processes outlined in our Social Networking Policy.

- Access to social networking sites will be filtered as appropriate.
- When access is needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the Headteacher.
- Pupils are regularly educated on the implications of posting personal data online.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and Endon Hall Primary & Nursery School as a whole. Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about Endon Hall Primary & Nursery School which may affect its reputation.
- Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the Headteacher prior to accessing the social media site.

18. Use of Smart technology and devices

Mobile devices are not permitted to be used during school hours by pupils or staff unless authorised by the Headteacher. Staff are permitted to access phones in the classroom setting in order to receive a two-factor authentication code linked to their Office365 log-in, before the school day begins.

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's 'Acceptable Use Agreement' for Pupils.

Staff will use all smart technology and personal technology in line with the school's 'Acceptable Use Policy' for Staff.

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access in the school office.

The Headteacher may authorise the use of mobile/smart devices by a pupil where it is seen to be for safety or precautionary use.

Where a pupil uses accessibility features on a personal device to help them access education e.g. where a pupil who is deaf uses their mobile phone to adjust the settings on an internal hearing aid in response to audible stimuli during class, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.

Staff are permitted to use hand-held computers which have been provided by Endon Hall Primary & Nursery School, though internet access will be monitored by the Online Safety Coordinator for any inappropriate use when using these on the school premises.

The sending of inappropriate messages or images from mobile devices is prohibited.

All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

Mobile devices must not be used to take images or videos of pupils or staff, without the prior agreement of the Headteacher/SLT.

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers
- Sharing indecent images, both consensually and non-consensually
- Viewing and sharing pornography and other harmful content

Pupils will not be permitted to wear or use smart devices, watches, or any other personal technology whilst in school.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

19. Online hoaxes and harmful online challenges

For the purposes of this policy, an “**online hoax**” is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, “**harmful online challenges**” refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

The DSL/Online Safety Lead ensures that pupils are taught about how to critically identify when online content is untrue or harmful and how to respond to this content.

The DSL will work with the SENDCo to assess whether some pupils e.g. pupils who have been identified as being vulnerable or pupils with SEND, need additional help with identifying harmful online challenges and hoaxes, and tailor support accordingly.

The school will ensure all pupils are aware of who to report concerns to surrounding potentially harmful online challenges or hoaxes e.g. by displaying posters, messages in assemblies/as part of theme weeks. This applies to concerns reported both in and out of school, where concerns out of school are brought to the attention of the school and/or are impacting on children in school.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL/Online Safety Lead will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country.

Where the harmful content is prevalent mainly in the local area, the DSL/Online Safety Lead will consult with the LA/Trust about whether quick local action can prevent the hoax or challenge from spreading more widely.

The DSL/Online Safety Lead will check the factual basis of harmful online challenges or hoaxes against a known, reliable and trustworthy source e.g. the UK Safer Internet Centre, and will carefully consider if a challenge or story is a hoax or is harmful prior to providing any direct warnings to pupils or parents.

The school understands that discussing or naming a specific online hoax can, in some cases, needlessly increase pupils' exposure to distressing content, and will avoid showing pupils distressing content where doing so is not considered absolutely necessary for preventing its spread or easing fears amongst the school community.

Where the DSL/Online Safety Lead's assessment finds an online challenge to be putting pupils at risk of harm e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The DSL/Headteacher/Online Safety Lead will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL/Headteacher/Online Safety Lead will decide whether each proposed response is:

- Factual and avoids needlessly scaring or distressing pupils
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it e.g. where content is explained to younger pupils that is almost exclusively being shared amongst older pupils
- Proportional to the actual or perceived risk
- Helpful to the pupils who are, or are perceived to be, at risk
- Age-appropriate and appropriate for the relevant pupils' developmental stage
- Supportive
- In line with other sections of this policy

20. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact that pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the Internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the Internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy. Advice will be sought from the Safeguarding Advice Team wherever necessary.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil, relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

21. Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the schools Social, Emotional and Mental Health (SEMH) & Well-being layered/targeted approach.

A weekly Online Safety Drop-in session will be available for children to access support from the Online Safety coordinator.

22. Generative artificial intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

23. Educating Parents/Carers

The school will work in partnership with parents/carers to ensure pupils stay safe online at school and at home.

Parents/carers will be provided with information about the school's approach to online safety and their role in protecting

their children. Parents/carers will be sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents/carers will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming
- Exposure to radicalising content
- Sharing of indecent imagery of pupils e.g. sexting
- Cyberbullying
- Exposure to age-inappropriate content e.g. pornography
- Exposure to harmful content e.g. content that encourages self-destructive behaviour

Parents/carers will be informed of the ways in which they can prevent their child from accessing harmful content at home e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how to support children to be safe online will be raised in the following ways:

- School website; Newsletters; Online resources & signposting; Facebook posts (National Online Safety resources)

Appendix 1

Endon Hall Primary & Nursery School

'Inspire today to achieve tomorrow'



Incident sheet for users to report any actual/potential online safety incident to the Online Safety Lead

Date and time of report/incident	
Location of report/incident/online activity (website/platform)	
Technology being used when incident occurred	
Program being used (if relevant/known)	
Name of individual(s) involved	
Name of member of staff reporting incident	

Please give a description below of the nature of concern/incident you are reporting to the Online-Safety Lead
(including any pertinent background information that may assist in understanding the concern and/or previous reports/incidents related to the individuals involved):

--

Action taken/follow up required by Online Safety Co-ordinator (detail any immediate actions taken in response to the concern e.g. notifying parents/carers, providing guidance to relevant pupils, and/or reporting to relevant authorities)

--

* This form should also be submitted to the designated safeguarding lead as soon as possible following the report of an online safety concern.

Appendix 2

Endon Hall Primary & Nursery School

'Inspire today to achieve tomorrow'



Requests for website release

Website release being requested	
Member of staff requesting the release	

Please give a description below of how this website will be used in the classroom and how this will have a positive impact on the children's learning.

--

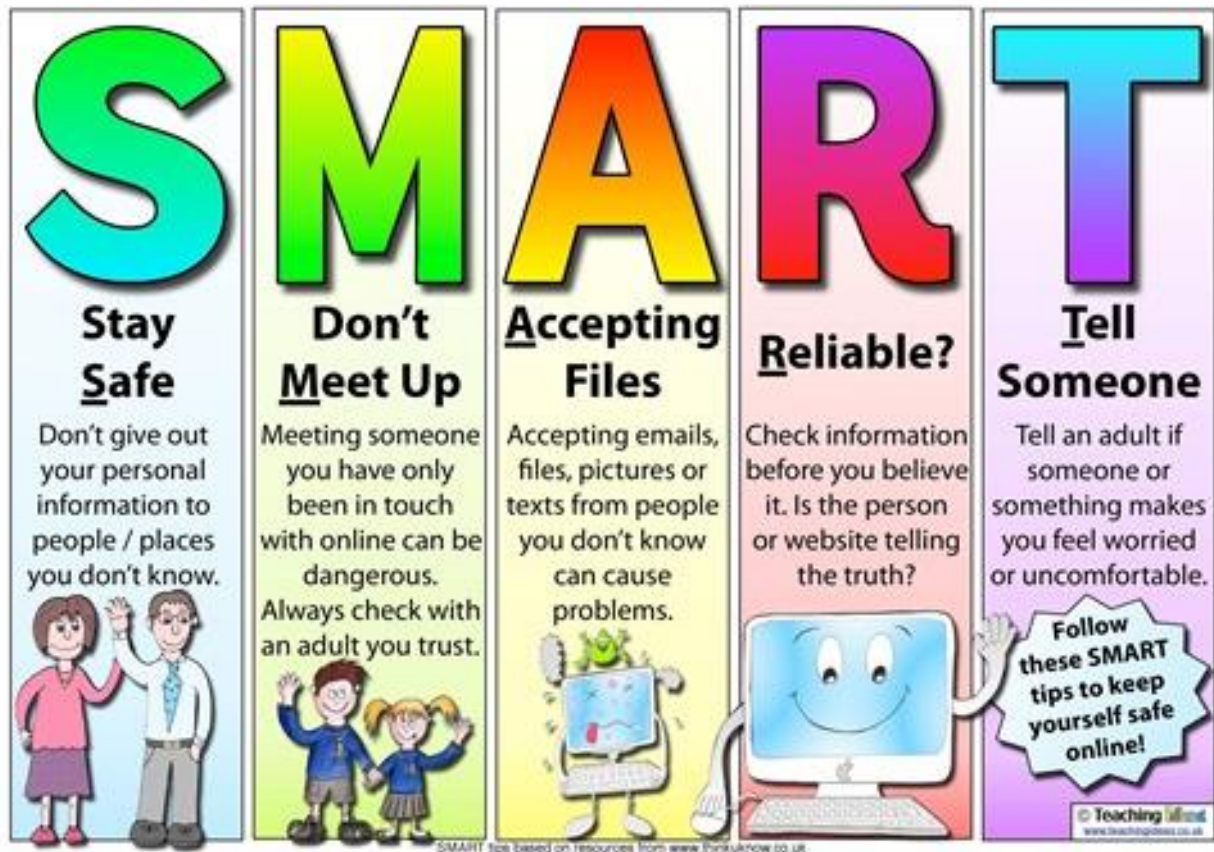
Signed: (member of staff requesting the website release) _____ Date: _____

Signed: (Online-Safety Co-ordinator) _____ Date: _____

Request accepted/rejected?

Date: _____ Signed: _____

Appendix 3



Appendix 4



Self-image and identity

This strand explores the differences between online and offline identity beginning with self-awareness, shaping online identities and how media impacts on gender and stereotypes. It identifies effective routes for reporting and support and explores the impact of online technologies on self-image and behaviour.



Online relationships

This strand explores how technology shapes communication styles and identifies strategies for positive relationships in online communities. It offers opportunities to discuss relationships and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.



Online reputation

This strand explores the concept of reputation and how others may use online information to make judgements. It offers opportunities to develop strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles.



Online bullying

This strand explores bullying and other online aggression and how technology impacts those issues. It offers strategies for effective reporting and intervention and considers how bullying and other aggressive behaviour relates to legislation.



Managing online information

This strand explores how online information is found, viewed and interpreted. It offers strategies for effective searching, critical evaluation and ethical publishing.



Health, well-being and lifestyle

This strand explores the impact that technology has on health, well-being and lifestyle. It also includes understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.



Privacy and security

This strand explores how personal online information can be used, stored, processed and shared. It offers both behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.



Copyright and ownership

This strand explores the concept of ownership of online content. It explores strategies for protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.