Endon Hall Primary & Nursery School

'Learning together and having fun'

Online Safety Policy

Policy in place: Sept 2016 **Reviewed:** July 2021 **Review date:** July 2022

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

Contents:

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 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 three 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.

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'

This policy also has regard to the following statutory guidance:

- DfE (Sept 2018) 'Keeping Children Safe in Education'

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 Head Teacher 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.
- 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 Health & Safety Committee receiving regular information about online safety incidents and monitoring reports. The Online Safety Governor representative is TBC.

The role of the Online Safety Governor will include:

- Regular meetings with the Online Safety Co-ordinator
- 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.

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 Coordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. Monitoring will 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 monitoring reports from the Online Safety Co-ordinator.

- The Headteacher and Acting 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).

Online safety Coordinator

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

Technical staff

The Computing Co-ordinator 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 Co-ordinator/Headteacher/Deputy Headteacher/Acting 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 Co-ordinator/Headteacher/Deputy Headteacher/Acting 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.

Designated person for child protection

The Designated and Deputy Designated Child Protection officers will be trained in and keep up to date with developments in online safety issues, remaining aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Potential radicalisation

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

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.

- 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 Co-ordinator and will be reviewed, at least 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 Co-ordinator 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 Co-ordinator.
- 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 appropriately 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 School in the following ways:

- A planned online safety programme will be provided and delivered in Computing sessions, as part of our Computing Scheme of Work. It will be regularly revisited. This will cover both the use of ICT and new technologies in school and outside school.
- The curriculum and the school's approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance.
- 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

- Planned sessions will include (Appendix 4);
    - Underpinning knowledge and behaviours (evaluating online behaviour, online relationships)
    - Harms and risks (Online relationships, Privacy and Security, Online reputation, Online bullying, Managing online information, copyright and ownership)
    - Wellbeing (Self-image and identity, Online reputation, Online bullying, Health, wellbeing and lifestyle)
- 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 on-line 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 and 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 on-line experiences. Parents 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 web site
- School Facebook page
- Parents evenings/meetings
- Other events e.g. family learning events

Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff.
- An audit of the online safety training needs of all staff will be carried out regularly.

- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Policies, and all other related policies.
- The Online Safety Coordinator will receive regular updates through attendance at Local Authority/other information/training sessions and by reviewing guidance documents released by the LA and others.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings/INSET days.
- The Online Safety Coordinator will provide advice/guidance/training to individuals as required.

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.

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 activities in lessons and out of school. 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 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. 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			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in 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.

12. 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.

13. 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.

14. 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.

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					✓	
On-line gaming (educational)				✓		
On-line gaming (non-educational)					✓	
On-line gambling					✓	
On-line shopping / commerce			✓			
File sharing				✓		
Use of social networking sites					✓	
Use of video broadcasting e.g. YouTube			✓			

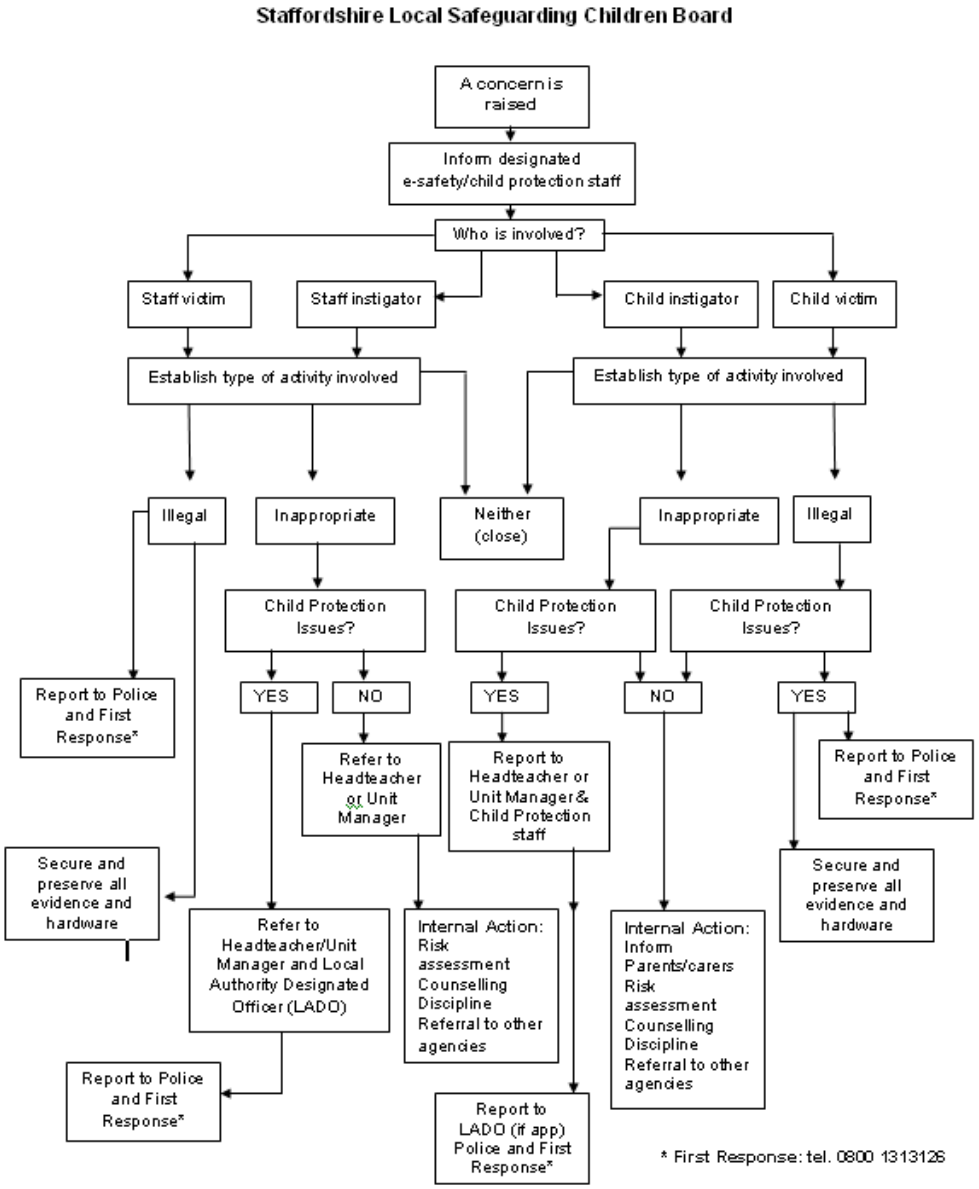
15. Responding to incidents of misuse

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– below and http://www.staffsscb.org.uk/Professionals/Key-Safeguarding/online safety/online safety-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.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the contact 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.

Peer-on-Peer Abuse

The school recognises that peer-on-peer abuse can take place online. Examples include the following:

- Non-consensual sharing of sexual images and videos
- Sexualised cyberbullying
- Online coercion and threats
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

The school responds to all concerns regarding online peer-on-peer abuse, whether or not the incident took place on the school premises or using school-owned equipment.

Concerns regarding online peer-on-peer abuse are reported to the DSL who will investigate the matter in line with the Child Protection and Safeguarding Policy.

Information about the school's full response to incidents of online peer-on-peer abuse can be found in the Child Protection and Safeguarding Policy.

Upskirting

Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person's clothing without consent and with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose.

A "specified purpose" is namely:

- Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear)
- To humiliate, distress or alarm the victim

"Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge e.g. a motion activated camera.

Concerns/reports regarding upskirting are reported to the DSL who will investigate the matter in line with the Child Protection and Safeguarding Policy.

16. Social networking and personal publishing

Use of social media on behalf of Endon Hall 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, outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and Endon Hall Primary 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 School which may affect its reputability.
- 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.

17. Mobile devices and hand-held computers

Mobile devices are not permitted to be used during school hours by pupils or staff unless authorised by the Headteacher.

The Headteacher may authorise the use of mobile 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 School, though internet access will be monitored for any inappropriate use by the Online Safety Coordinator when using these on the school premises.

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

Mobile devices must not be used to take images or videos of pupils or staff.

18. 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.

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

Appendix 1

Endon Hall Primary & Nursery School

'Learning together and having fun'

Incident sheet for users to report any actual/potential online safety incident to the Online Safety Co-ordinator.

Date and time of incident	
Location of incident	
Technology being used when incident occurred	
Program being used (if known)	
Name of member of staff reporting incident	

Please give a description below of the incident you are reporting to the Online-Safety co-ordinator.

Signed (member of staff reporting the incident): _____ Date: _____

Action taken by Online Safety Co-ordinator:

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

Appendix 2

Endon Hall Primary & Nursery School

'Learning together and having fun'

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.

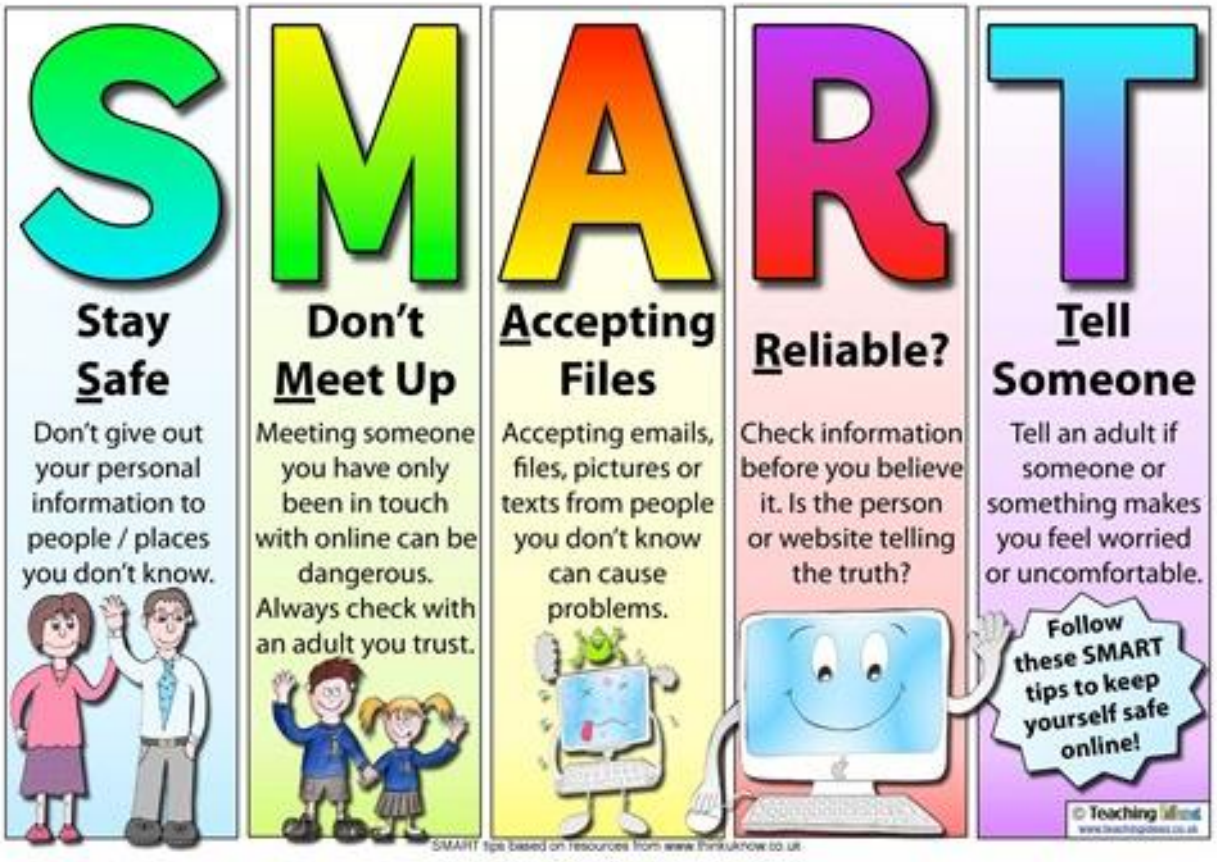
Signed: (member of staff requesting the website release) _____ Date: _____

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.