Endon Hall Primary School

'Learning together and having fun'

Online Safety Policy

Policy in place: Sept 2016 **Policy reviewed:** Sept 2017 **Review date:** Sept 2018

	Member of staff responsible	Governor	Senior member of staff
Online Safety	Miss A Coleman	Ms C 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. Communications
12. Data protection
13. Unsuitable / inappropriate / illegal activities
14. Responding to incidents of misuse
15. Social networking and personal publishing
16. Mobile devices and hand-held computers
17. Appendix

1. Introduction

At Endon Hall Primary 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 children 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 children and staff.

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

Legal framework

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

- The Human Rights Act 1998
- The Data Protection Act 1998
- 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

This policy also has regard to the following statutory guidance:

- DfE (2015) 'Keeping Children Safe in Education'

2. Aims

- To actively provide and promote opportunities for developing children's 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 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

4. School Website

The contact details on the website show the school address, e-mail and telephone number. Staff or children's 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 children will be selected carefully and will not enable individual children to be clearly identified without the prior consent of the child's parent/carer.
- Children's full names will not be used anywhere on the website, particularly in association with photographs.

- Written permission from parents/carers will be obtained before photographs of children are published on the school website.
- Permission may be requested from a child's parent/carer, before their work will be considered for publication on the school website.

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 Ms C Soboljew.

The role of the Online Safety Governor will include:

- Annual meetings with the Online Safety Co-ordinator
- Monitoring/awareness of Online Safety incident logs
- Reporting to relevant Governors' committee

Headteacher and Senior Leaders

- The Headteacher has overall responsibility 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 will support those in school who carry out the internal online safety monitoring role.
- 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 annually 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.

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 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 children (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.
- Children understand and follow the school Online Safety and Acceptable Use Policy.
- Children 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 children 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

Children

- Are responsible for using the school IT systems in accordance with the Child Acceptable Use Policy which is provided at the start of their time at the school. Parents/carers may sign on behalf of their child/ren.
- 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, the school website and information about national/local online safety campaigns/literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Child Acceptable Use Policy.
- Accessing the school website in accordance with the relevant school 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 Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. locked filing cabinet in school office). The school will never allow one user to have sole administrator access.
- Users will be made 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 children to share their partner's log-on.
- The school maintains and supports the managed filtering service (NetSweeper) 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 use Impero software to 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 (e.g. memory sticks/CDs/DVDs) by users on school workstations/portable devices (see School Personal Data Policy).
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured (see School Personal Data Policy).

7. Online safety Education and Training

Children

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children in online safety is therefore an essential part of the school's online safety provision. Children 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 (termly) as part of our Computing Scheme of Work and/or through PSHE/other lessons. It will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key online safety messages will be reinforced as part of a planned programme of assemblies and learning activities.
- Children 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.
- Children will be helped to understand the need for the child AUP and encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside school.
- Children 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 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 website
- 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.
- 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 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, children 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 children are allowed to freely search the internet e.g. using search engines, staff will be vigilant in monitoring the content of the websites the children visit.
- It is accepted that from time to time, for good educational reasons, children 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).
- Children 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
- Children 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 children instant use of images that they have recorded themselves or downloaded from the internet. However, staff and children 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 children 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. Childs 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, on the school website and occasionally in the public media.
- Care will be taken when taking digital/video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Childs must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere, that include children, will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents/carers will be obtained before photographs of children are published on the school website (consent form signed by parents/carers at the start of the year).

10. Cyber Bullying

Opportunities for children 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 children about appropriate behaviours when using technology provides a vital grounding for future use. Whilst not wanting to provoke unrecognised opportunities in children, 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).
- Children, parents/carers, staff and governors will all be made aware of the consequences of cyber-bullying.
- Children and their parents/carers will be made aware of a child's 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/carers.
- The school will take all reasonable precautions to ensure against cyber-bullying whilst children 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.

The school will proactively engage with children 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 kept and will be 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				Children			
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 children 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 children 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.

- Children 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 Data Protection Act 1998 which states that personal data must be:

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

Staff must ensure that they:

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

When personal data is stored on any portable computer system, USB stick or any other removable media, at least one of the following must apply:

- The data must be encrypted and password protected.
- The device must be password protected (some memory sticks/cards and other mobile devices cannot be password protected).
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

13. 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 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		✓			

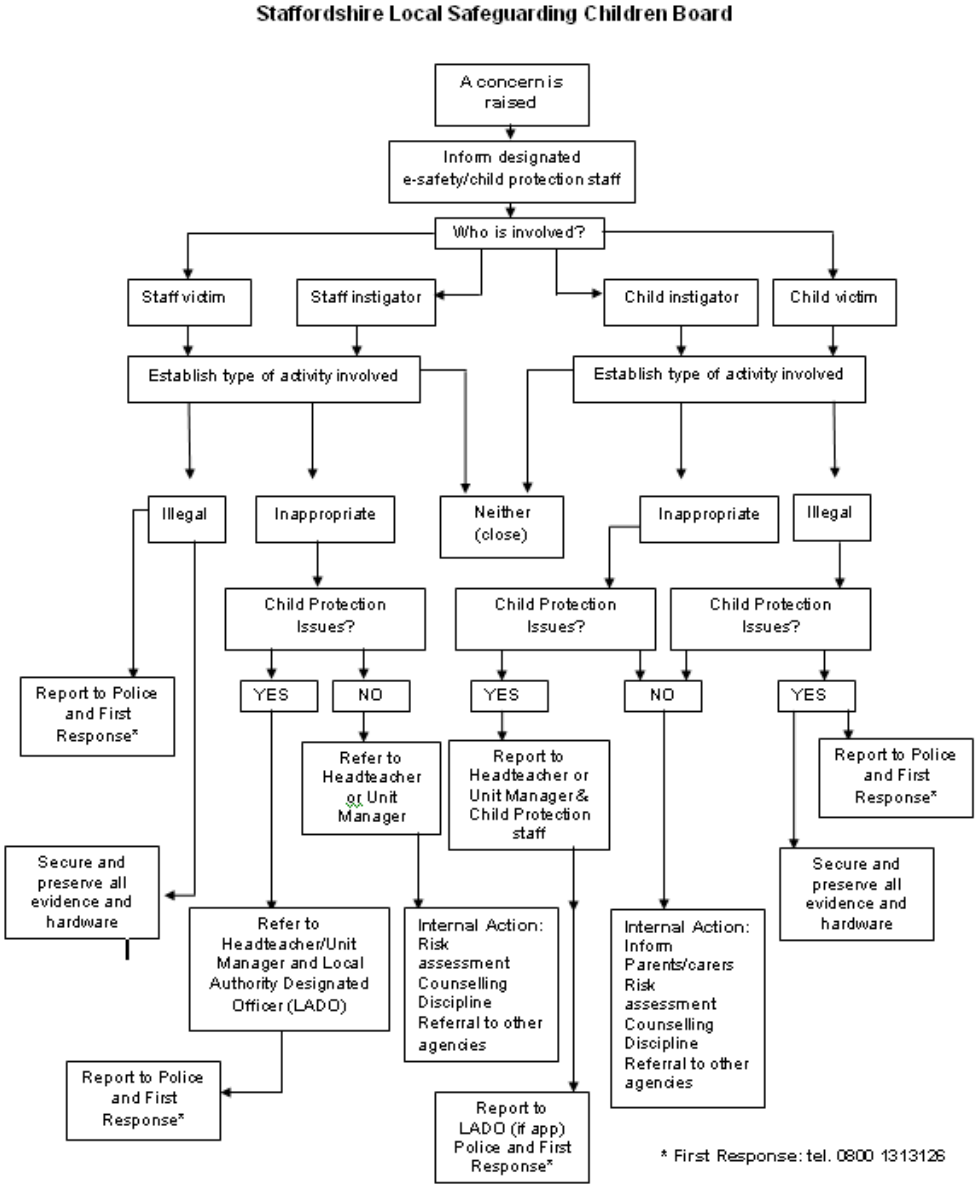
14. Responding to incidents of misuse

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.

15. Social networking and personal publishing

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

- Access to social networking sites will be filtered as appropriate.
- Should access be 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.
- Children 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 children 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.

16. Mobile devices and hand-held computers

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

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

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.

Personal devices must not be used to take images or videos of children or staff.

Appendix 1

Endon Hall Primary 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 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.

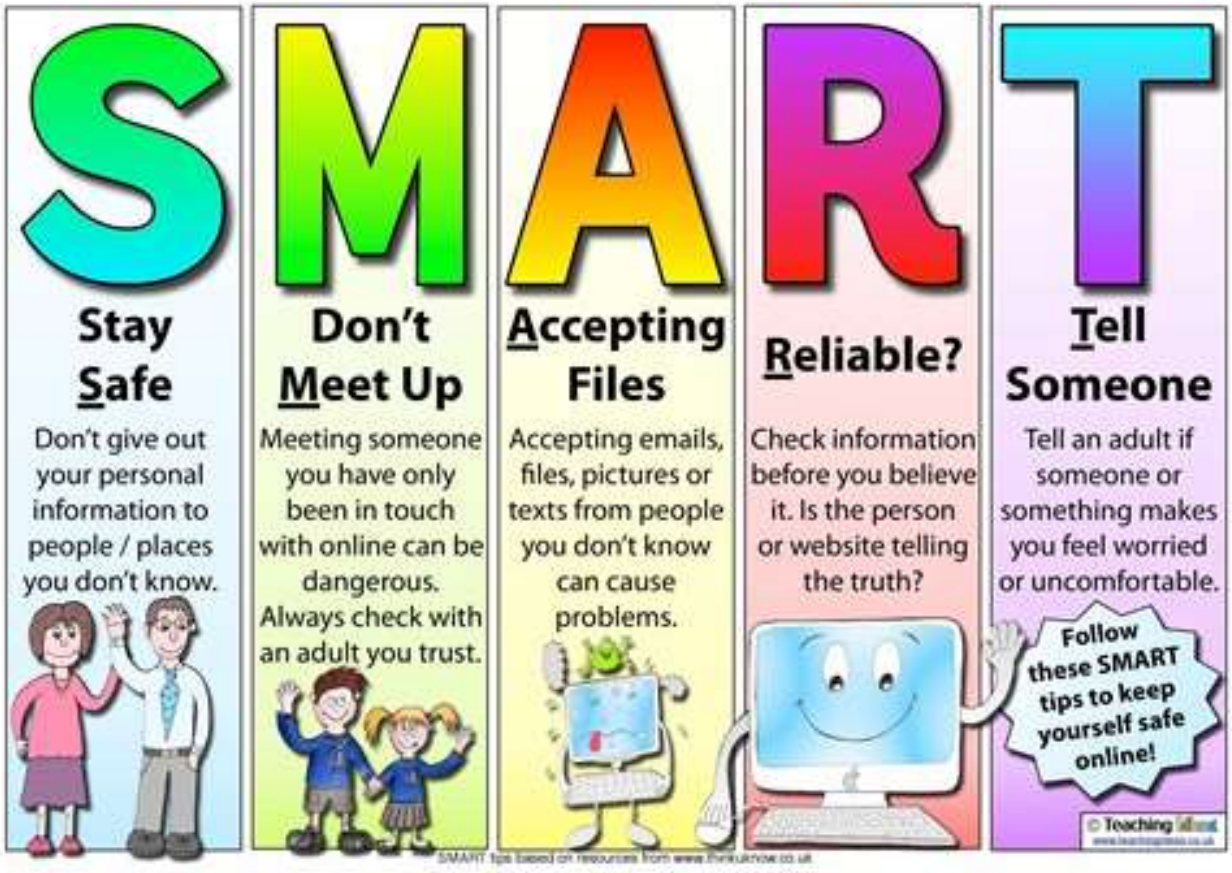
Signed: (member of staff requesting the website release) _____ Date: _____

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

Request accepted/rejected?

Date: _____ Signed: _____

Appendix 3


S
Stay Safe
Don't give out your personal information to people / places you don't know.
M
Don't Meet Up
Meeting someone you have only been in touch with online can be dangerous. Always check with an adult you trust.
A
Accepting Files
Accepting emails, files, pictures or texts from people you don't know can cause problems.
R
Reliable?
Check information before you believe it. Is the person or website telling the truth?
T
Tell Someone
Tell an adult if someone or something makes you feel worried or uncomfortable.
Follow these SMART tips to keep yourself safe online!
© Teaching
SMART tips based on resources from www.thinkuknow.co.uk