West Haddon Endowed CE Primary School

ACCEPTABLE USE POLICY

‘Where Happiness Promotes Success’

OUR SCHOOL VISION

To ensure every child leaves our school with an outstanding education and the values and character to live life in its fullness, contributing positively to society.

Jesus said: I have come in order that you might have life-and life in all its fullness. John 10:10

Produced in consultation with
Staff, Governors, Parents and School Council

1. Policy Statement

IT and the internet have become integral to teaching and learning within schools; providing children and staff with opportunities to improve understanding, access online resources and communicate with the world, all at the touch of a button. At present, internet-based technologies used extensively by young people in both home and school environments include:

- Websites and Search Engines
- Social Media
- Mobile Phones
- Tablets and other developing devices with wireless technology.
- Online Gaming
- Music Downloading
- Learning Platforms and Visual Learning Environments
- Email, Instant Messaging, Video Messaging and Chat Rooms.
- USBs and Transferable Storage (e.g. CDs, DVDs, Memory Sticks)
- Podcasts
- Artificial Intelligence (AI)

The use of technology within school and at home increased considerably due to the pandemic of Covid-19 and has continued since. This has added more opportunities for adults and children but this has also added more risks and challenges too.

While this technology has many benefits for our school community, we recognise that clear procedures for appropriate use and education for staff and pupils about online behaviours, age restrictions and potential risks is crucial.

At West Haddon Endowed C. of E. Primary School, we have a duty to ensure that pupils are protected from potential harm both within and beyond the school environment. Every effort will be made to safeguard against all risks, however it is unlikely that we will be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure that pupils and staff continue to be protected. In accordance with Ofsted requirements, young people need to be empowered and educated to make healthy and responsible decisions when using the internet, in particular, social media.

2. Why have an Acceptable Use Policy?

The use of technology and the internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children access these technologies. The risks include:

- Children accessing inappropriate content.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Cyber-bullying, child-on-child abuse and stalking.
- Sexting - the sending of indecent personal images, videos or text via mobile phones and other similar/developing devices for private viewing. Can potentially be widely distributed and publicly viewed.
- On-line content which is abusive or pornographic
- Radicalisation
- Trolling (on-line harassment and negative / bullying comments)
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or any mobile device.
- Viruses.
- Commercial issues with spam and other inappropriate e-mail.
- Disinformation, misinformation and conspiracy theories.
- AI content to spread disinformation, misinformation and conspiracy theories.

It is also important that adults are clear about the procedures so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks. Staff are trained annually in Online Safety and reminded of the risks children and staff face, key people and reporting concerns process (CPOMs and which concerns need direct police involvement).

Whilst the school or setting should acknowledge that every effort will be made to safeguard against all risks, it is likely that they will never be able to completely eliminate them. Any incidents that may arise should be dealt with quickly and according to policy to ensure children and young people continue to be protected.

It is our duty to take all reasonable steps to ensure that children and young people are protected from potential harm both within and beyond the school environment. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of on-line technologies. The term 'online safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

3. Aims

- To ensure the safeguarding of all children and staff at West Haddon Endowed C. of E. Primary School by detailing appropriate and acceptable use of all online technologies.
- To outline the role and responsibility of everyone in the school community.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.
- To develop links with parents/carers and the wider community, ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technology.

4. Roles and Responsibilities of the School:

4.1 Governors and Head teacher

It is the overall responsibility of the Head teacher, with the Governors, to ensure that there is an overview of online safety (as part of the wider remit of Child Protection) across the school with further responsibilities as follows:

- The Head teacher has a designated Online Safety Leader to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring Online Safety is addressed in order to establish a safe digital learning environment. All staff and students are aware of who holds this post within the school.
- Time and resources should be provided for the Online Safety Leader to update the policy annually and for the Online Safety Leader and staff to be trained, when such training arises.
- The Head teacher is responsible for promoting online safety across the curriculum and has awareness of how this is being developed, linked with the school development plan.
- The Head teacher should inform the Governors about the progress of any updates to the online safety curriculum (via PSHE or Computing) and ensure Governors know how this related to Child Protection.
- The Head teacher or designated Online Safety Leader will inform the Child Protection Governor of any misuse or incident relating to online safety.
- Any temporary unblocking of filters within the school must be sanctioned by the Head teacher.
- The Governors must ensure Child Protection is covered with an awareness of online safety and how it is being addressed within the school, as it is the responsibility of the Governors to ensure that all Child Protection guidance and practices are embedded.
- Governors must challenge the school about having an Acceptable Use Policy with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT, including challenging the school about having:
    - Filters
    - Firewalls
    - Antivirus and antispyware software
    - Using an accredited Internet Service Provider
    - Awareness of wireless technology issues.
    - A clear policy on using personal devices.
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures (see the Allegation Procedure – Section 1 of Local Safeguarding Children's Board Northamptonshire) and appropriate action is taken, even to the extreme of suspending a member of staff, informing the Police (via agreed protocols with the Police) or involving parents/carers. See appendices for example procedures on misuse.

The governor responsible for Online Safety is Kevin Montgomery.

4.2 Online Safety Leader

It is the role of the designated Online Safety Leader to:

- Appreciate the importance of online safety within school and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe Computing learning environment within the school.
- Ensure that the AUP is reviewed annually, with up-to-date information available for all staff to teach online safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff, children and young people, in the initial set up of a network, stand-a-lone PC, staff/children laptops, chrome books and tablets and the learning platform (Google Classroom) or ensure the technician is informed and carries out work as directed.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Head teacher as issues arise.
- Liaise with the PSHE, Child Protection and Computing Leaders so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct e-safety information can be taught or adhered to.
- Keep a log of incidents, alongside a member of the Designated Safeguarding Team for analysis to help inform future development and safeguarding, where risks can be identified. Refer to Section 12 of the Allegation Procedure from the NSCB to ensure the correct procedures are used with incidents of misuse (website in Appendices).
- Keep an up-to-date record of staff acceptable user forms.
- Work alongside the Computing Leader, to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops, chrome books and tablets and that this is reviewed and updated on a regular basis.
- Ensure that ICT technicians can check for viruses on laptops, stand-a-lone PCs, chrome books, tablets and memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensure that unsolicited e-mails to a member of staff from other sources is minimised by limiting who has the email addresses to those only connected with educational backgrounds or purposes. Refer to section 12 of the Allegation Procedure, NSCB, for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.

The Online Safety Leader is Joanna Foster.

4.3 Staff or adults

It is the responsibility of all adults within the school or other setting to:

- Ensure that they know who the Designated Safeguarding People for Child Protection are within school, so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it should be reported immediately to the Head teacher. In the event of an allegation made against the Head teacher, the Chair of Governors must be informed immediately. (Following the Allegation Procedure, Section 12, NSCB.)
- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event

that a procedure is unknown, they will refer to the Head teacher immediately, who should then follow the Allegations Procedure, Section 12, NSCB, where appropriate.

- Report any concerns regarding filtering and access to technologies to the Online Safety Leader.
- Alert the Online Safety Leader of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children and young people should know what to do in the event of an incident.
- Follow the Online Safety Long Term Curriculum Plan.
- Be up-to-date with e-Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Sign an Acceptable User Form to show that they agree with and accept the rules for staff using non-personal equipment, within and beyond the school environment, as outlined in appendices.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998 and in-line with General Data Protection Regulations 2018.
- Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- School bursars will need to ensure that they follow the correct procedures for any data required to be taken from the school premises.
- Report accidental access to inappropriate materials to the Online Safety Leader and Internet Service Provider (Easi-PC) helpdesk in order that inappropriate sites are added to the restricted list or control this with the Local Control options via your broadband connection.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis, especially when not connected to the school/educational setting's network.
- Ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.
- Report incidents of Online Safety issues or inappropriate behaviours on CPOMs.
- Members of Staff are expected to ensure their laptop / tablet is secure for access when unattended.

4.4 Children

Children and young people are:

- Responsible for following the Acceptable Use Rules whilst within school as agreed at the beginning of each academic year or whenever a new child attends the school for the first time. At the beginning of the year each child will be expected to sign the rules and this will be displayed within the classroom. These are also sent home and the children will discuss and sign with their adult.
- Taught to use the internet in a safe and responsible manner through Computing, PSHE or other cross curricular links. Online safety lessons will be taught four to six times spread across the year, as well as a learning unit and additionally as the need arises.
- Responsible for using their own login and no-one else's as well as ensuring they log off correctly after use.

- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).
- Are aware of what to do if something they access on the internet or other devices are offensive or upsetting (see appendices for a copy of our rules)

4.5 ICT Technician Team

The ICT Technician Team is responsible for ensuring:

- That the ICT infrastructure in school is secure and not open to misuse or malicious attack.
- That anti-virus software is installed and maintained on all school laptops, machines and portable devices.
- That the school's filtering policy is applied and updated on a regular basis and that the responsibility for its implementation is shared with the Online Safety Leader and the Designated Person for Safeguarding.
- That any problems or faults relating to filtering are reported to the Designated Person for Safeguarding and to the broadband provider immediately and recorded on the Online Safety Incident Log.
- That users may only access the school's network through rigorously enforced password protection, in which passwords are regularly changed.
- That they keep up to date with online safety technical information in order to maintain the security of the school network and safeguard children.
- That the use of the school network is monitored in order that any deliberate or accidental misuse can be reported to the Online Safety Leader.

5. Appropriate Use

5.1 By Staff:

- Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.
- They have a password to access a filtered internet service and know that this should not be disclosed to anyone.
- All staff receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Form which needs to be signed and returned to the school office, to be copied and filed.
- The Acceptable Use Rules (on the Acceptable Use Form) will be displayed in the staffroom to remind the need to safeguard against potential allegation. Staff training should underpin this policy.

Any inappropriate use must be reported to the Head teacher / Online Safety Lead immediately and then the Allegations Procedure (Section 12, NSCB) and the Child Protection Policy must be followed to deal with any misconduct. All appropriate authorities must be contacted. In the lesser event of misuse or accidental misuse, refer to appendices for a list of actions relating to the scale of misuse.

5.2 By Children:

The Acceptable Use Rules for children will be sent as a letter to parents/carers at the start of each school year (see appendices). These detail how children are expected to use the internet and other technologies within school or other settings. The rules are there for children to understand what is expected of their behaviour and attitude when using ICT, which enables them to take responsibility for their own actions. For example, knowing what is polite to write to another child in e-mails, texts, social networks etc. and understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequence for doing so. These rules will also be signed by the children at school and displayed in the classrooms. It also outlines the use of Google Classroom both at home and at school.

School encourages parents/carers to support the rules and discuss them with their child. This can be shown by signing the Acceptable Use Rules together so that it is clear to the school that the rules are accepted but the child with the support of the parent/carer. Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at the time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

Support and information for parents/carers will be accessible and sent out regularly and as and when needs / issues arise.

Should a child be found to misuse the ICT facilities whilst at school, the following consequences (which are reviewed annually) should occur:

- Any child found to be misusing the internet by not following the Acceptable Use Rules may have their parents/carers contacted, explaining the reason for suspending the child for a particular lesson / or activity.
- Further misuse of the rules may result in not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers.
- A letter may be sent to parents/carers outlining the breach in Child Protection Policy where a child or young person is deemed to have misused technology against another child or adult.
- If serious abuse of the internet continues then a letter should be sent home informing parents of a permanent suspension will be implemented and the reasons why.

In the event that a child accidentally accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, e.g. close the device lid or lock the screen, so that an adult can take the appropriate action. Where a child feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or deliberately misusing on-line technologies should also be addressed by the school.

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

6. Children with additional learning needs

We strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a pupil has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of online safety lessons and internet access.

7. The Curriculum and Tools for Learning

Using the Internet is part of the curriculum and is a fantastic and necessary tool for learning. It is part of everyday life for education, business and social interaction. The school has a duty in providing pupils with quality internet access as part of their learning experience.

West Haddon Endowed C. of E. Primary School teaches children how to use the internet safely and responsibly through the curriculum. They are taught through Computing, PSHE and other lessons how to research information, explore concepts and communicate effectively in order to further learning.

At school, pupil usage of the internet is monitored and supervised by the school filtering system – Securly. Pupils use the internet widely out of school and need to learn how to use it safely, evaluate information for themselves and take responsibility for their safety and experience.

Online safety is part of the Computing and PSHE curriculum and is an ongoing learning process. The school uses resources from online safeguarding programmes from CEOP (think u know) as well as from the South West Grid for Learning and through the Purple Mash scheme of work.

7.1 Internet Use

We teach our children how to use the internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding, and communicating effectively in order to further learning skills. The following concepts, skills and competencies should have been taught by the time children leave Year 6:

- Digital literacy
- making good judgements about websites and e-mails received
- knowledge of risks such as viruses and opening mail from a stranger
- access to resources that outline how to be safe and responsible when using any on-line technologies
- knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content
- uploading information – know what is safe to upload and not upload personal information
- where to go for advice and how to report abuse

- clickbait and unsafe links online
- managing screen time effectively
- digital footprints
- password protection
- risks of social media / age expectations
- gender stereotypes
- cyber bullying
- self-image and identity
- online reputation
- health and well-being
- AI and deepfake

7.2 Personal Safety

Ensuring information uploaded onto websites and e-mailed to other people does not include any person information, including:

- Full name
- Address
- Telephone number
- E-mail address
- School
- Clubs attended and where.
- DOB or age
- Routes to and from school.
- Any information which would make it easy for a stranger to identify a child or locate their whereabouts (e.g. number 8 in the football team)

The children are also taught about the importance of personal safety.

Children are also taught about social media. Although many of the apps and social media sites have an age limit which is above primary school age, many of the children do access these so it is important to ensure they are educated on the risks and dangers these can pose. Children learn about potential issues, including:

- people not being who they say they are.
- unknown individuals 'following' or 'becoming friends' online.
- using the correct privacy settings to ensure profiles are private.
- trolling comments and videos.
- how to report inappropriate behaviour and comments.
- how apps can track your location.
- how many apps work on algorithms and push content based on your previous views

Photographs from school should only be uploaded on the approval of a Designated Safeguarding Person or parent/carer and should only contain something that would be acceptable in 'real life'. Parents/carers should monitor the contents of photographs uploaded.

7.3 Email Use

Children now have school email addresses, linked to Google Classroom and so that they are able to login to the Chromebooks. Children learn about safe email use through their online safety lessons.

Although they use the emails help them to login to the Chromebooks and Google Classroom, they do not access the email app within school.

Staff are issued their own school email addresses for any communication between home and school as well as contacting outside agencies.

7.4 *Learning Platform* –

Since the outbreak of Covid-19, the school continues to use Google Classroom both within the classroom and also for the children to complete home learning if children have to work from home for any reason.

Google Classroom allows for children to:

- access work and resources set by adults in real time.
- use links to aid their learning.
- upload their work.
- meet in video conferencing with their peers and adults from school safely.
- communicate with adults from school to ask questions about the work.
- Be part of an online community.

Children are taught about how to use Google Classrooms safely and appropriately by their class teacher and during their online safety lessons.

Children and young people should use their login and password to access the internet via Google Classroom so that the level of filtering is appropriate. Our school filtering system is designed so that children should not be able to access content that is inappropriate to them.

Staff or adults need to ensure they consider the risks and consequences of anything they or their children and young people may post to any web or social networking sites, as inappropriate comments or images can reflect poorly on an individual and can affect future careers.

7.5 *Mobile Phones (and other emerging technologies)*

(i) Children are not currently permitted to have their mobile phones in school or on school trips. If they are walking to school and have their mobile phone with them for safety, they must enter school via the office and leave their phone there. They may only collect it when leaving the school premises before going home.

(ii) Staff are allowed to bring in personal mobile phones or devices for their own use, but must not use personal numbers to contact children / pupils under any circumstances. It is the responsibility of the staff member to ensure that there is no illegal or inappropriate content stored on their device when brought onto school grounds. If staff choose to contact parents via their personal mobile devices (in circumstances such as working from home or for parents evening via phone), they must use 141 to withhold their number beforehand.

(iii) Devices must be in silent mode or switched off during school hours and should not be checked for personal messages while teaching is in progress.

(iv) Any mobile phones which connect to the school Wi-Fi system is subjected to the same level of filtering as staff laptops and sites accessed whilst on the school Wi-Fi will be monitored.

(v) Staff should be aware that games consoles such as Sony PlayStation, Microsoft Xbox, Nintendo Switch and other such systems have internet access which may not include filtering. Before use within school, authorisation should be sought from the Head teacher and the activity supervised by a member of staff at all times.

(vi) The school is not responsible for the loss, theft or damage of any personal devices including mobile phones.

(vii) Children are not permitted to have tracking devices in school or on school trips. Tracking devices brought into school must be left in the school office (stored in a Faraday box).

7.6 <u>School issued mobile devices</u>

The management of the use of these devices should be similar to those stated above, but with the following additions: Where the establishment has provided a mobile device to a member of staff, such as a laptop, iPad, tablet, PDA or mobile phone, this equipment should only be used to conduct school business outside of the school environment.

It should also be policy to ensure that children understand the use of a public domain and the consequences of misuse. Relevant curriculum links should be made to highlight the legal implications and the involvement of law enforcement. Other technologies within schools used with children and young people include:

- Photocopiers
- Telephones
- PDAs
- Ipads / Ipods
- Chrome books
- Tablets
- Smart watches
- Any other similar emerging devices.

7.7 <u>Videos and Photographs</u>

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone. When in school there is access to: laptops with cameras, digital cameras, flip cams and web cams.

It is also highly recommended that permission is sought prior to any uploading of images to check for inappropriate content.

The sharing of photographs via weblogs, forums or any other means on-line should only occur after permission has been given by a parent/carer or member of staff.

Photographs/images used to identify children and young people in a forum or using Instant Messaging within the learning platform should be representative of the child rather than of the child e.g. an avatar.

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website. Photographs should only ever include the child's first name although Child Protection Guidance states either a child's name or a photograph but not both.

Group photographs are preferable to individual children and young people and should not be of any compromising positions.
During community events, parents are informed of the possible dangers and expectations when taking pictures of their children. They are asked to crop images to only contain their child if they plan to upload any images online.

7.8 Video-conferencing and webcams

- Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.
- Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school setting. This process should always supervised by a member of staff and a record of dates, times and participants held by the school.
- Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Rules.)
- Where children, young people (or adults) may be using a webcam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable Use Rules.
- When using the meet feature on Google Classrooms a number of steps must be taken to ensure the safety of both adults and children. These include:
    - i) Google Meet feature turned off until scheduled meet time.
    - ii) Google Meet code to be reset after each meet in case children have copied it and could therefore access it without a member of staff present.
    - iii) Two adults employed by the school to be in every video meet OR the whole meeting to be recorded.
    - iv) Children asked to have their cameras on and be in a communal area of their house (i.e. not in their bedroom).
    - v) Children and adults to be dressed appropriately for the meet sessions.
    - vi) Parents asked to be off screen once the child is set up for the meet.

8. Monitoring

School technical staff, the Online Safety Lead and members of the Senior Leadership Team monitor user activity, including any personal use of the school IT system. This is done on a regular basis and is recorded, filed and kept in a specific file in the large Teacher's office.

8.1 School IT Equipment

- A log of all IT equipment issued to staff, including serial numbers, is maintained by the school.
- Personal or sensitive data will not be stored on school devices unless password protected.

8.2 Personal devices

- Children are not permitted to bring mobile phones into school or on trips (see section 7.5). If children walk to and from school with a mobile phone, they are to take it to the office at the start of the school day and collect it at the end.

- Staff mobile phones – see section 7.5. Any mobile phones which connect to the school Wi-Fi system is subjected to the same level of filtering as staff laptops and sites accessed whilst on the school Wi-Fi will be monitored.

8.3 *Laptops / iPads*

- Staff must ensure that all sensitive school data is stored on password protected devices. In the event of loss / theft or failure to safeguard sensitive data could result in a serious security breach and subsequent action will be taken.
- Personal use of school laptops and equipment, whilst onsite is left to the discretion of the Head teacher and may be permissible if kept to a minimum, used outside lesson time and does not interfere with the employees' work.
- Staff are provided with laptops to allow for school related work to be completed offsite. Personal use of the laptop from home (such as web browsing / online shopping etc) is permitted but should be kept to a minimum and use of the device is strictly restricted to the authorised member of staff (i.e. not family members)
- Staff are aware that all activities carried out on school devices and systems, both within and outside of the school environment, will be monitored in accordance with this policy.
- Staff will ensure that school laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring / servicing.

9. Web 2.0 Technologies.

9.1 *Managing Social Networking and other Web 2.0 Technologies.*

Social networking sites have emerged as a leading method of communication proving increasingly popular amongst both adults and young people alike. The service typically offers users both a public and private space through which they can engage with other online users, and expresses themselves creatively through images, web content and their own personal profile page. With responsible use, this technology can assist with the development of key social skills whilst also providing users with access to a range of easily accessible, free facilities. However, as with any technology that opens a gateway to online communication with young people, there are a number of risks associated which must be addressed. With this in mind, both staff and pupils are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published (examples of which include Facebook, Instagram, Snapchat, Tiktok, Threads, Twitter, and BeReal.) In response to this issue the following measures should be put in place:

- Access to social networking sites, such as Facebook, Instagram, Twitter, Snapchap etc. are not permitted to be accessed on school equipment.
- Students are advised against giving out personal details or information which could identify them or their location (e.g. mobile phone number, home address, school name, groups or clubs attended, social media handles, IM and email address or full names of friends.)
- Students are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Advice is also given regarding background images in photos which could reveal personal details (e.g. house number, street name, school uniform)

- Pupils are advised on social networking security and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
- The school should be aware that social networking can be a vehicle for cyber bullying. Pupils are encouraged to report any incidents of bullying to the school allowing for the procedures, as set out in the anti-bullying policy, to be followed.

9.2 *Social Networking Advice for Staff*

- Social networking outside of work hours, is the personal choice of all school staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:
    - Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
    - Staff should not engage in personal online contact with students outside of Head teacher authorised systems (e.g. school email account for homework purposes). This includes parents messaging staff over sites such as Facebook Messenger. If this happens, staff should not reply and should report this to the Head teacher.
    - Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
    - Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students)

10. Safeguarding Measures

10.1 *Filtering*

We have now been using Securly since October 2024 for our filtering and monitoring system. For the 2024 academic year, we will begin to use Securly as our new filtering and monitoring system. This is provided via our technical provider – Easi-PC. This monitors usage on all devices connected to the system / internet and flag any inappropriate usage. A report is provided to the DSL and Online Safety Leader regularly as well as flagging up anything that needs to be investigated immediately.
Securly works to protect users from harmful AI, while recognising that it has a place in schools when used appropriately.

Anti-virus and anti-spyware software is used on all network and stand-alone PCs or laptops and is updated on a regular basis by the ICT technicians.

Children should be encouraged to use a search engine that is age appropriate such as Google Kids, Swiggle or Safe Search UK or Yahooligans. At present children are permitted to use Google, although there can be some unsavoury materials embedded within the Google Images tabs that all staff are

aware of. Should any instances arise that cause a safety issue, Google will be added to the black list, ensuring this site cannot be used.

Links or feeds to e-safety websites are provided.
Children are taught to close the lids of the Chromebooks so that anything accidentally accessed can be hidden whilst an adult is informed.

For older children and young people, the Report Abuse button is available should there be a concern of inappropriate or malicious contact made by someone unknown. This provides a safe place for children and young people to report an incident if they feel they cannot talk to a known adult.

CEOP (Child Exploitation and On-line Protection Centre) training for secondary children and young people (and Year 6 Primary children) is annual and part of the PSHE curriculum for raising awareness on staying safe and being responsible. A link to the www.thinkukknow.co.uk website is part of the skin layout for further advice and information on children's or young people's personal on-line spaces. Encryption codes on wireless systems prevent hacking.

10.2 *Tools for bypassing filters*

- Students and staff are forbidden to use any technology designed to circumvent, avoid or bypass any school or educational setting's security controls (including internet filters, antivirus solutions or firewalls.) as stated in the Acceptable Use Rules.
- Violation of this rule should result in disciplinary or in some circumstances legal action. Please refer to the 'Staff Procedures Following Misuse by Staff/Children and Young People' sections of this document.

10.3 *Incident Reporting*

- Staff to CPOMs if an issue arises of concern.

11. Parents

11.1 *Roles*

Whilst there is no statutory requirement for parents to sign acceptable use policies, evidence shows that children and young people signing agreements to take responsibility for their own actions, is successful. Each child or young person should receive a copy of the Acceptable Use Rules on an annual basis or first-time entry to the school which need to be read with the parent/carer, signed and returned to school confirming both an understanding and acceptance of the rules.
It should be expected that parents/carers will explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.
School should keep a record of the signed forms.

11.2 *Support*

As part of the approach to developing e-safety awareness with children and young people, the school may offer parents the opportunity to find out more about how they can support the school or setting in keeping their child safe and find out what they can do to continue to keep them safe

whilst using on-line technologies beyond school. The school promotes a positive attitude to using the World Wide Web and therefore wants parents to support their child's learning and understanding of how to use on-line technologies safely and responsibly.

The Appendices detail where parents/carers can go for further support beyond the school. The school should endeavour to provide access to the internet for parents/carers so that appropriate advice and information can be accessed where there may be no internet at home, subject to arrangement.

12. Links to other policies

12.1 *Behaviour and Anti-Bullying Policies*

Please refer to the Behaviour Policy and Anti-bullying Policy for the procedures in dealing with any potential bullying incidents via any on-line communication, such as mobile phones, e-mail, gaming chats, via social media, text / WhatsApp or blogs. This School has an up to date Anti-bullying Policy which will include any cyber bullying issues. All behaviours should be seen and dealt with in exactly the same way, whether on or off-line and this needs to be a key message which sits within all Computing and PSHE materials for children and young people and their parents/carers. People should not treat on-line behaviours differently to off-line behaviours and should have exactly the same expectations for appropriate behaviour. This is a key message which should be reflected within Behaviour and Anti-bullying Policies as it is only the tools and technologies that change, not the behaviour of children, young people and adults.

12.2 *Managing allegations and concerns of abuse made against people who work with children.*

Please refer to the Allegation Procedure, Section 12 LSCB, in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies. The procedures detail how to deal with allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations made against a member of staff should be reported to the DSL immediately. In the event of an allegation being made against a Head teacher, the Chair of Governors should be notified immediately.

12.3 *Health and Safety Policy*

Refer to the Health and Safety Policy and procedures of the school/setting and the County Council for information on related topics, particularly Display Screen Equipment, Home working and Accident/Incident reporting procedures. Wireless technologies are not considered to be a hazard following advice from the Health Protection Agency to the Government.

12.4 *School website*

The uploading of images to the school website should be subject to the same acceptable rules as uploading to any personal on-line space. Permission ought to be sought from the parent/carer prior to the uploading of any images. Settings should consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

12.5 *External websites*

In the event that a member of staff finds themselves or another adult on an external website, such as 'Rate My Teacher', as a victim, schools/settings are encouraged to report incidents to the Headteacher and unions, using the reporting procedures for monitoring.

12.6 Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of on-line technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

13.Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and speed on-line) or 'cyber-dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include:

- Unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded;
- Denial of Service (Dos or DDoS) attacks or 'booting'. These attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and,
- Making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including above.

Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, the designating safeguarding lead (or a deputy), should consider referring to the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Note that Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.
Additional advice can be found at Cyber Choices, NPCC – When to call the Police and National Cyber Security Centre (NCSC.gov.uk).

14. The 4Cs

In Keeping Children Safe in Education (KCSIE), It states that it is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

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

• **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

• **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

• **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

• **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Appendices

Staff Procedures Following Misuse by Staff

The Head teacher will ensure that these procedures are followed, in the event of any misuse of the internet, by an adult:

A. An inappropriate website is accessed inadvertently:
   Report website to the Online Safety Leader if this is deemed necessary.
   Log on the monitoring system.
   Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned or restricted list. Change Local Control filters to restrict locally.
   Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
   Ensure that no one else can access the material by shutting down.
   Log the incident.

Report to the Head teacher and Online Safety Leader immediately.
Head teacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
Inform the LA/RBC filtering services as with A.

C. An adult receives inappropriate material.
Do not forward this material to anyone else – doing so could be an illegal activity.
Alert the Head teacher immediately.
Ensure the device is removed and log the nature of the material.
Contact relevant authorities for further advice e.g. police.

D. An adult has used ICT equipment inappropriately:
Follow the procedures for B.

E. An adult has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately, if necessary.
Report to the Head teacher and Designated Safeguarding Lead for Child Protection immediately, who should then follow the Allegations Procedure and Child Protection Policy from Section 12, NSCB.
Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Head teacher to implement appropriate sanctions.
If illegal or inappropriate misuse is known, contact the Head teacher or Chair of Governors (if allegation is made against the Head teacher) and Designated Safeguarding Lead for Child Protection immediately and follow the Allegations procedure and Child Protection Policy.
Contact CEOP (police) as necessary.

F. Threatening or malicious comments are posted to the school website or learning platform (or printed out) about an adult in school:
Preserve any evidence.
Inform the Head teacher immediately and follow Child Protection Policy as necessary.
Inform the RBC/LA/LSCB and e-Safety Leader so that new risks can be identified.
Contact the police or CEOP as necessary.

G. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Head teacher.

Staff Procedures Following Misuse by Children and Young People

The Head teacher will ensure that these procedures are followed, in the event of any misuse of the internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:
Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.

Report website to the Online Leader if this is deemed necessary.
Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned list or use Local Control to alter within your setting.
Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
Refer the child to the Acceptable Use Rules that were agreed.
Reinforce the knowledge that it is illegal to access certain images and police can be informed.
Decide on appropriate sanction.
Notify the parent/carer.
Inform LA/RBC as above.

C. An adult or child has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately.
Report to the Head teacher and Designated Safeguarding Lead for Child Protection immediately.
Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
If illegal or inappropriate misuse the Head teacher must follow the Allegation Procedure and/or Child Protection Policy from Section 12, NSCB.
Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website or learning platform about a child in school:
Preserve any evidence.
Inform the Head teacher immediately.
Inform the RBC/LA/NSCB and e-Safety Leader so that new risks can be identified.
Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in the school or setting:
Preserve any evidence.
Inform the Head teacher immediately.

N.B. There are three incidences when you must report directly to the police.

Indecent images of children found.

Incidents of 'grooming' behaviour.

The sending of obscene materials to a child.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found.
They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine.

Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image.

- www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line.

Procedures need to be followed by the school within Section 12 of the Allegations Procedure and Child Protection Policy from the Northamptonshire Safeguarding Children's Board guidance.

All adults should know who the Designated Safeguarding Lead for Child Protection is.

It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the internet or E-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

These rules apply to all on-line use and to anything that may be downloaded or printed.

- I know that I should only use the school equipment in an appropriate manner.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
- I have read the Procedures for Incidents of Misuse (appendices of Acceptable Use Policy) so that I can deal with any problems that may arise, effectively.
- I will report accidental finding of inappropriate materials so that appropriate action / blocking can be taken.
- I will report any incidents of concern for children's or young people's safety to the Head teacher, Designated Safeguarding Lead for Child Protection or Online Safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Designated Safeguarding Lead for Child Protection is and other members of the DST.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail and social media. I should use the school E-mail and phones (wherever possible) and only to a child's school E-mail address as part of the curriculum.
- I know that I should not be using the school network (and hardware in school) for personal use unless this has been agreed by the Head teacher and/or Online Safety Leader.
- I know that virus checks will be completed on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone requests my password I will check with the Online Safety Leader.
- I will use Google Classroom appropriately and only contact children via this in accordance to the rules in the Acceptable Use Policy. I accept this will be monitored.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass school filtering systems is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures for staff misuse.
- I have been given a copy of the Acceptable Use Policy to refer to about all online safety issues and procedures that I will adhere to.
- I understand that all activity online is monitored regularly.
- I will take care not to spread misinformation, disinformation and conspiracy theories and I will look at information online objectively.

Signed (staff member/governor/volunteer/visitor):	**Date:**

EYFS and KS1 acceptable use agreement (pupils and parents/carers)

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

When I use the school's ICT systems (like Chromebooks) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I select a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Carry the Chrome Books and other ICT equipment carefully and how I have been taught.
• Log off or shut down a computer when I have finished using it
• Know that adults from school will not contact me outside of school except on whole class Google Classroom posts or work feedback if I have been using Google Classroom at home.
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

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

KS2 acceptable use agreement (pupils and parents/carers)

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

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

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

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it
- Know that adults from school will not contact me outside of school except on whole class Google Classroom posts or work feedback if I have been using Google Classroom at home.

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless an adult has given me permission.
- Open any attachments in emails, or follow any links in emails, without first checking with an adult
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is inappropriate and not related to my age.
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

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

- I will take it straight to the school office when I arrive in school and collect it at the end of the school day.
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

EYFS, Year 1 and 2

Our Online Safety and Chromebook Rules!

- ✓ We use the Chromebooks and other devices to help us learn.
- ✓ We listen to adults when using our devices and the internet.
- ✓ We treat the Chromebooks with respect by:
    - Always carrying them carefully, with two hands.
    - Plugging them back in to charge after we have used them.
    - Being gentle opening and closing and when using the touch screen and keyboard.
- ✓ We know how to keep ourselves safe online by regularly learning about Online Safety and remembering it when we go online.
- ✓ We know to keep personal information private, including:
    - Not sharing our last name.
    - Not sharing where we live (our address).
    - Keeping the school and any clubs we go to private.
    - Not sharing our birthday with people we don't know.
    - Keeping our passwords to ourselves and a trusted adult.
- ✓ We know to always be polite and kind online, just as we would be to people face to face.

- ✓ We know to say no if anything makes us feel uncomfortable and to tell a trusted adult when something doesn't feel right or if we are worried.
- ✓ We know that not everything we see online is true.
- ✓ We know how to search safely online and that websites such as www.swiggle.org.uk are good for children my age to use.
- ✓ We know who we can go to for help if we are stuck or feeling worried online.

We pledge to follow our school Online Safety and Chromebook Rules!

Year 3, 4, 5 and 6

Rules!

- ✓ We treat the Chromebooks with respect by:
  - Always carrying them carefully, one at a time, with two hands.
  - Plugging them back in to charge after we have used them.
  - Being gentle opening and closing and when using the touch screen and keyboard.
- ✓ We use the Chromebooks and Google Classroom to help us with our learning.
- ✓ We know how to keep ourselves safe online by regularly learning about Online Safety and remembering it when we go online.
- ✓ We know to keep personal information private, including:

- Not sharing our last name, our address, our school and clubs, our birthday, email address or social media handles with people we don't know.
- Keeping our passwords to ourselves and a trusted adult and we know how to make strong passwords.
- Not sharing photographs or video clips without permission.

✓ We know how to communicate politely, kindly and safely online.
✓ We know our trusted adults who can help us if we are uncomfortable online.
✓ We know other ways to report things online.
✓ We know not to communicate online with people we don't know and how to deal with it if someone unfamiliar contacts us.
✓ We know people aren't always who they say they are.
✓ We know that not everything we see online is true and how to fact check.
✓ We know we leave a digital footprint with everything we do online.
✓ We know how to search safely online and use search engines such as www.swiggle.org.uk

We pledge to follow our school Online Safety and Chromebook Rules!

www.thinkuknow.co.uk
(for all children and young people with a section for parents/carers and adults – this also links with the CEOP (Child Exploitation and On-line Protection Centre work)

www.netsmartzkids.org
(5 – 17)

www.hectorsworld.com
(for FS, Yr 1 and 2 and is part of the thinkuknow website above)

www.dcsf.gov.uk

(for adults)

www.becta.org.uk
(advice for settings to update policies)

https://www.westnorthants.gov.uk/directory/local-offer/d0d39856-e2ff-4b89-a897-4b9337e66c1a (Local Safeguarding Children West Northamptonshire

https://www.saferinternet.org.uk/advice-centre/parents-and-carers
(Information from the National Safer Internet site for parents and carers)

https://www.saferinternet.org.uk/advice-centre/young-people
(Information, games, quizzes etc. for children and young people on Safer Internet use – ages 3-11 and 11-19)

https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff
(for materials for teachers and professionals)

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
(NSPCC information for adults on e-safety)

How UK Schools Can Support Safe, Responsible AI Use in Education Securly filtering and monitoring information on AI in schools.

Generative AI: product safety expectations - GOV.UK Government information on Generative AI.