The Abbey Primary School

Online Safety Policy

Approved by:	Emma Killick HT	**Date:** 1st September 2025
Last reviewed on:	September 2025	
Next review due by:	September 2026	

Contents

1. Policy Aims

- This online safety policy has been written by The Abbey Primary School, with guidance, specialist advice and input as required.
- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2025, Early Years and Foundation Stage Framework 2025, 'Working Together to Safeguard Children' 2025 and the Northamptonshire Safeguarding Children Board procedures.
- The purpose of The Abbey Primary School online safety policy is to:
    - Safeguard and protect all members of The Abbey Primary School community online.
    - Identify approaches to educate and raise awareness of online safety throughout the community.
    - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns.
- The Abbey Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:
    - **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
    - **Contact:** being subjected to harmful online interaction with other users, for example: child-onchild 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:** 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.

2. Policy Scope

- The Abbey Primary School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- The Abbey Primary School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life, and believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide

services on behalf of the setting (collectively referred to as “staff” in this policy) as well as learners, parents and carers.

- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.2 Links with other policies and practices

This policy links with several other policies, practices and action plans, including:

- Anti-bullying Policy
- Acceptable Use Policy
- Social Policy
- Child protection and safeguarding Policy
- Whistleblowing policy
- Curriculum policies, such as: Computing, Personal Social and Health Economic (PSHE), Relationships and Sex Education (RSE)
- Data Protection Policy
- Staff Code of Conduct

3. Monitoring and Review

- Technology in this area evolves and changes rapidly. The Abbey Primary School will review this policy at least annually.
- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the headteacher will be informed of online safety concerns, as appropriate.
- Where relevant, the Online Safeguarding Lead in conjunction with the named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

- Overall, the ultimate lead responsibility for safeguarding and child protection, including online safety, remains with The Abbey Primary School Designated Safeguarding Lead, Emma Killick, Headteacher.

- The Online Safeguarding Lead (OSL), Emma Killick, has responsibility for overseeing online safety, with some directed and monitored activities delegated to the computing team. Online safety will be managed, alongside safeguarding and child protection, in conjunction with members of the DSL team.
- The Abbey Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including an Acceptable Use Policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Alongside the Computing Leads, ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the OSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.

4.2 The Online Safeguarding Lead (OSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside the DSL team and deputy OSLs, to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.

- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Report online safety concerns, as appropriate, to the DSL/ SLT.
- Work with the SLT to review and update online safety policies on a regular basis (at least annually).
- Regular communication with the governor with a lead responsibility for safeguarding/online safety.

4.3 It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the Online Safety Policy and Acceptable Use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.

  Embed online safety education across curriculum delivery, wherever possible.
- Teach and embed online safety lessons through PSHE and computing lessons using the identified PSHE curriculum and the Teach Computing Curriculum.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Follow clear guidance on when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the OSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures including, but not exclusive to, antivirus software, filtering and encryption, as directed by the leadership team to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.

- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure appropriate access and technical support is given to the OSL to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

4.5 It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age-appropriate online safety education opportunities.
- Read and adhere to the Acceptable Use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and carers to:

- Read the Acceptable Use policies and encourage their children to adhere to them.

  Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.

  Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement and Acceptable Use policies.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with learners

- The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
  - Ensuring education regarding safe and responsible use precedes internet access.
  - Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study. EYFS should follow the EYFS Statutory Guidance and incorporate discussions about online safety when

modelling and using a range of technology, as well as taking part in whole school events, such as Safer Internet Day. All KS1 and KS2 year groups will be taught using The Computing Hub Scheme of work.

- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation. ○ Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The setting will support learners to read and understand the Acceptable Use policies in a way which suits their age and ability by:
  - Displaying Acceptable Use posters in all rooms with internet access.
  - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
  - Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
  - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.
  - Take part in National and local online safety events where appropriate.

5.2 Vulnerable Learners.

- The Abbey Primary School recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- When implementing an appropriate online safety policy and curriculum The Abbey Primary School will seek input from specialist staff as appropriate, including the SENDCo, to ensure identified children are supported.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will be included as a part of existing safeguarding and child protection training/updates and within separate annual online safety sessions. It will cover the potential risks posed to learners (Content, Contact, Conduct and Commerce) as well as our professional practice expectations.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- The Abbey Primary School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, through social media and the school website, and through relevant publications distributed throughout the academic year.
    - Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
    - Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.

- Requiring them to read our Acceptable Use policies and discuss the implications with their children.

6. Reducing Online Risks

- The Abbey Primary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
  - Regularly review the methods used to identify, assess and minimise online risks.
  - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
  - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
  - Recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology 7.1

Classroom Use

The Abbey Primary School uses a wide range of technology. This includes access to:

- Laptops, tablets and other digital devices
- Internet which may include search engines and educational websites
- Email
- Digital cameras, web cams and video cameras

All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

The school employs EasiPC to manage and monitor iPads across the school.

Securly filtering are applied with individual server logins. Cloud based reports are available for access and regular spot monitoring, or to access a support with any online safety investigations.
All devices are required to use a proxy server when using the setting Wi-Fi.

Securly send a weekly report to the OSL with any usernames that have flagged up any concerning keystrokes word and phrase captures. A full in-depth report can be accessed on the cloud software for each username, including which program the user was accessing. DSLs also receive email alerts regarding any attempts to access blocked content or websites have taken place.

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

The setting will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.

When pupils are using search engines, ensure they are using KidRex https://www.alarms.org/kidrex/ or Google Safe Search https://www.safesearchkids.com

To minimise risk, when using Google image search as a teaching tool, ensure that the screen is not visible to students until results have been vetted.

We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.

Supervision of learners will be appropriate to their age and ability.

Early Years Foundation Stage and Key Stage 1

Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.

Key Stage 2

Learners will use age-appropriate search engines and online tools.

Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

7.2 Managing Internet Access

- All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

7.3 Filtering and Monitoring

7.3.1 Decision Making

- The Abbey Primary School governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks, taking into consideration advice from https://www.saferinternet.org.uk/advicehttps://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoringcentre/teachers-and-school-staff/appropriate-filtering-and-monitoring
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed on advice from EasiPC in guidance with current legislation and available software, considering our specific needs and circumstances.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- Education broadband connectivity is provided through EXA.
- We use Securly which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming, social media, adult and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- We work with Securly and EasiPC to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
    - Close the laptop or turn over the iPad and report the concern immediately to a member of staff.
    - The member of staff will report the concern (including the URL of the site if possible) to the OSL (or deputy) and/or technical staff.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Northamptonshire Police or CEOP.

7.4. Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
    - Securly filtering software and cloud log information.
    - User and IP linked logins linked to the tracking and monitoring software.
    - EasiPC monitor and supervise iPad use.
    - Physical supervision by staff when pupils are using any internet connected device.
- If a concern is identified via monitoring approaches:
    - A OSL or deputy will respond in line with the child protection policy.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.5 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

7.6 Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly.
    - Encryption for personal data sent over the Internet or taken off site, including encrypted memory sticks.
    - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments.

- Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network.
  - Specific user logins and passwords will be enforced for all but pupils in EYFS and identified learners with specific SEND requirements.
- All users are expected to log off or lock their screens/devices if systems are unattended.

7.6.1 Password policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From Year 1 all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to:
  - Use strong passwords for access into our system.
  - Always keep their password private; users must not share it with others or leave it where others can find it.
  - Not to login as another user at any time.

7.7 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.8 Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: Online Safety, Image Use, Data Protection, Acceptable Use, Staff Code of Conduct, and Mobile Phones policies.

7.9 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the staff code of conduct.

    - The forwarding of any chain messages/emails is not permitted.
    - Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
    - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell the OSL and the DSL team if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Access to external personal email accounts may be blocked on site.
- Any emails containing sensitive information will not contain any full names and should use initials only wherever possible.

7.9.1 Staff email

- The use of personal email addresses by staff for any official setting business is not permitted.
    - All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

7.9.2 Learner email

- Learners will use provided email accounts for educational purposes, when age and skills appropriate.
- Learners will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the setting.

7.10 Management of Programmes used to Record Children's Progress

- We use iTrack, Pixl and Ruth Miskin (RWI) to track learners' progress.
- The headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:
    - Only learner issued devices will be used for programs that record and store learners' personal details, attainment or photographs.
    - Personal staff mobile phones or devices will not be used to access or upload content to any programs which record and store learners' personal details, attainment or images.
    - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.

- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.

7.11 Management of Online Learning Platforms

The Abbey Primary School uses ***Microsoft Teams*** as its official learning platform.

- Leaders and staff will regularly monitor the usage of the Online Learning Platform, including message/communication tools and publishing facilities.
- Only current members of staff and learners will have access.
- When staff and learners leave the setting, their account will be disabled.
- Learners and staff will be advised about acceptable conduct and use and will be expected to adhere to all guidance in the Online Safety Policy, the Acceptable Use Policy, Image Use Policy and Computing Policy.
- All users will be mindful of copyright and will only upload appropriate content.
- Any concerns about content will be recorded and dealt with in the following ways:
    - Any material deemed to be inappropriate, or offensive will be removed.
    - Any breach of safeguarding or other cause for concern will be reported using My Concern, as well as informing DSLs and in accordance with other school policy where appropriate.
    - Access to the Online Learning Platform for the user may be suspended.
    - A learner's parents/carers may be informed.
    - If the content is illegal, we will respond in line with existing child protection procedures.

All online teaching and learning will be carried out in accordance with 2021 government guidance: https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19

8. Artificial Intelligence (AI)

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

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The Abbey Primary recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. The Abbey Primary will treat any use of AI to bully pupils in line with our Behaviour Policy. Staff should follow the INMAT Trust AI Policy and be aware of the risks of using AI tools whilst they are still being developed. Pupils will be taught the risks and benefits of using AI within the curriculum, particularly in Computing and Relationship Education.

9. Social Media

9.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of The Abbey Primary School community.
- The term social media may include (but is not limited to): blogs, social networking sites, forums; bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger.
- All members of The Abbey Primary School community are expected to engage in social media in a positive, safe and responsible manner.
    - All members are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- Learner and staff access to social media whilst using setting provided devices and systems on site will be blocked, unless otherwise agreed with the OSL.
    - Use of social media for personal use, whilst using setting devices during setting hours may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of The Abbey Primary School community on social media, should be reported to the DSL/OSL and will be managed in accordance with our Anti-Bullying, Whistleblowing, Staff Code of Conduct, and Child Protection policies.

9.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our staff code of conduct policy as part of the Acceptable Use policies.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
    - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.

    - Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of The Abbey Primary School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the headteacher immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.
- Any pre-existing relationships or exceptions that may compromise this, should be disclosed to the headteacher. If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use official setting provided communication tools.
- Staff will not use personal social media accounts to contact learners, parents, or families, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the headteacher.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL/headteacher.

9.3 Learners Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore learners will not create their own accounts.
- Any concerns regarding learners' use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
- Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.

- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.

9.4 Official Use of Social Media

The Abbey Primary School official social media channels are:

- https://www.facebook.com/The-Abbey-Primary-School-1681143982116651/ @theabbeyprimary
  https://twitter.com/TheAbbeyPrimary?ref_src=twsrc%5Etfw%7Ctwcamp%5Eembeddedtimeline%7Ctwterm%5Eprofile%3ATheAbbeyPrimary&ref_url=https%3A%2F%2Fwww.abbeyprimary.co.uk%2F @TheAbbeyPrimary
- www.abbeyprimary.co.uk
- https://www.instagram.com/theabbeyprimaryschool/ @theabbeyprimaryschool

- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
  - The official use of social media as a communication tool has been risk assessed and approved by the headteacher.
  - The Computing Team, SLT and the office staff have access to account information and login details for our social media channels.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
  - Setting provided email addresses to register for and manage any official social media channels.
  - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: Acceptable Use, Anti-Bullying, Image use, Data Protection, Confidentiality and Child Protection policies.
  - All communication on official social media platforms will be clear, transparent and open to scrutiny.
  - Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
  - We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels, and will make all information available on the school website and paper copies of important information are available.

Staff expectations

- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
  - Sign our social media acceptable use policy.

- Always be professional and aware they are an ambassador for the setting.
- Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure that they have appropriate consent before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, learners, parents and carers.
- Inform the headteacher or a member of the DSL team of any concerns, such as criticism, inappropriate content or contact from learners or families.

10. Use of Personal Devices and Mobile Phones

The Abbey Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

10.1 Expectations

- All use of personal devices, including but not limited to; laptops, tablets, smart watches and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, staff code of conduct, acceptable use, child protection and safeguarding policies.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
    - All members of The Abbey Primary School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
    - All members of The Abbey Primary School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used around the building whilst children are present, unless advised otherwise by SLT, during events such as, school performances or sporting events or if needed for medical reasons.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- All members of The Abbey Primary School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

10.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: Child protection and Safeguarding, Data Protection, Staff Code of Conduct and Acceptable Use.
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place during lesson time.
    - Keep mobile phones and personal devices, including smart watches and tablets switched off or switched to 'silent' mode during lesson times.
    - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
    - Not use personal devices during teaching periods, unless permission has been given by the headteacher, such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

  Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers. Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputy).
- Staff will not use personal devices:
    - To take photos or videos of learners and will only use work-provided equipment for this purpose.
    - Directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our Staff Code of Conduct and Whistleblowing policy.
    - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

10.3 Learners Use of Personal Devices and Mobile Phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- The Abbey Primary School does not permit learners' personal devices and mobile phones to be brought into the setting in Early Years to Year 4, except during exceptional circumstances, and in accordance with the Mobile Phone policy.
    - The parent/carer should write a the headteacher detailing the exceptional circumstances. If agreed the headteacher and parent/carer must complete an agreement in the form of a Pupil Mobile Phone Agreement.
    - Children in years 5 and 6 are permitted to bring a mobile device to school but must sign an agreement in the form of a Pupil Mobile Phone Agreement before they do.
    - The child should hand their device to their teacher in the morning, and it will be stored securely in the classroom. It can be collected at the end of the day.

- Mobile phones and personal devices will not be used by learners during the school day.
- If a learner breaches the policy, the parent/carer will be contacted, and this may affect agreement to allow the device to continue to be brought into the setting.
- Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our Social Policy or could contain youth produced sexual imagery (sexting).
- Learners' mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies in accordance with government guidance www.gov.uk/government/publications/searching-screeninghttp://www.gov.uk/government/publications/searching-screening-and-confiscationand-confiscation
- If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

10.4 Visitors' Use of Personal Devices and Mobile Phones

Parents/carers and visitors (including volunteers and contractors) are not permitted to use mobile phones and personal devices in the setting during school hours, with the exception of in the staff room, and/or meeting rooms if agreed with a member of the DSL team or SLT.

- Mobile device use permission may be granted at certain events, such as Christmas performances or sporting events, with a reminder of the Acceptable Use Policy agreement.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Visitors (including volunteers and contractors) who are on site for a regular or extended period will use their mobile phones and personal devices in accordance with our Acceptable Use Policy and other associated policies,
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or headteacher of any breaches our policy.

11. Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
- Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.

- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Northamptonshire Safeguarding Children Partnership and /or MASH team.
- Where there is suspicion that illegal activity has taken place, we will contact the Northamptonshire Safeguarding Children Partnership or Northamptonshire Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL will speak with Northamptonshire Police and/or Northamptonshire Safeguarding Children Partnership first to ensure that potential investigations are not compromised.

11.1 Concerns about a Learner's Welfare

- The OSL (or deputy) and DSL, or a member of the team, will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The OSL (or deputy) will record these issues in line with our child protection policy.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Northamptonshire Safeguarding Children Partnership thresholds and procedures.

  We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

11.2 Staff Misuse

- Any complaint about staff misuse will be referred to the headteacher, in accordance with the Whistleblowing policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the headteacher and /or INMAT where appropriate.
- Appropriate action will be taken in accordance with our staff code of conduct.

12. Procedures for Responding to Specific Online Incidents or Concerns

12.1 Online Sexual Violence and Sexual Harassment between Children

- Our setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2021) guidance and part 5 of 'Keeping children safe in education' 2025.
- The Abbey Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
- Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our Safeguarding Policy and Social Policy.

- The Abbey Primary School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- The Abbey Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- The Abbey Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE, RSE and online safety curriculum.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
    - If content is contained on learners' electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy.
    - Inform parents/carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as MASH and/or the Police.
    - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
    - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Northamptonshire Police first to ensure that investigations are not compromised.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

12.2 Youth Produced Sexual Imagery ("Sexting")

- The Abbey Primary School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'
- The Abbey Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods, delivered through the Teach Computing Curriculum.

- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
    - View any images suspected of being youth produced sexual imagery,
    - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
    - Act in accordance with our child protection policies and the relevant Northamptonshire Safeguarding Children Partnership procedures.
    - Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Store the device securely.
    - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
    - Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - Make a referral to MASH and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
    - Implement appropriate sanctions in accordance with our social policy but taking care not to further traumatise victims where possible.
    - Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
    - Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

12.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- The Abbey Primary School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

- The Abbey Primary School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our Safeguarding Policy and the relevant Northamptonshire Safeguarding Children Partnership protocols.
    - If appropriate, store any devices involved securely.
    - Make a referral to MASH (if required/appropriate) and immediately inform Northamptonshire police via 101, or 999 if a child is at immediate risk.
    - Inform parents/carers about the incident and how it is being managed.
    - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Northamptonshire Safeguarding Children Partnership and/or Northamptonshire Police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to MASH by the DSL (or deputy) http://www.northamptonshirescb.org.uk/tackling-child-sexual-exploitation-cse-/
- If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Northamptonshire Police and/or the Northamptonshire Safeguarding Children Partnership first to ensure that potential investigations are not compromised.

12.4 Indecent Images of Children (IIOC)

- The Abbey Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Northamptonshire Police and/or the Northamptonshire Safeguarding Children Partnership.
- If made aware of IIOC, we will:
    - Act in accordance with our Safeguarding Policy and the relevant Northamptonshire Safeguarding Children Partnership procedures.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Northamptonshire Police.

- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.

      Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the setting provided devices, we will:
    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and Northamptonshire Safeguarding Children Partnership (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
    - Report concerns, as appropriate to parents/carers.

- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
    - Ensure that the headteacher/DSL is informed in line with our Whistleblowing Policy and follow the relevant procedures.
    - Quarantine any devices until police advice has been sought.

12.5 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at The Abbey Primary School.
- Full details of how we will respond to cyberbullying are set out in our Behaviour Policy.

12.6 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at The Abbey Primary School and will be responded to in line with our Behaviour Policy.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through Northamptonshire Safeguarding Children Partnership services and/or Northamptonshire Police.

12.7 Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site, with the support of Securly filtering and monitoring.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our Safeguarding Policy and Prevent Duty legislation.
- If we are concerned that member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with the Safeguarding Policy and Prevent Duty legislation.

12.8 Sextortion

Sextortion is a type of blackmail in which an individual manipulates or threatens to distribute explicit or intimate material (such as sexual images or videos) of the victim, unless certain demands are met. Children and young people are often targeted through online platforms and social media. Sextortion is the short name for 'financially motivated sexual extortion'. Children and young people may be forced to pay money or do something else they do not want to.

- Staff members are aware that sextortion attempts can happen very quickly or they can happen over a long period of time. Where staff have a concern that a child is at risk of, or has been a victim of sextortion, this must be reported to the DSL immediately. This will be investigated in line with the Child Protection and Safeguarding Policy.

13. Useful Links for Educational Settings

Northamptonshire Support and Guidance for Educational Settings:

NCC:

- Simon Aston, Online Safety Officer for West Northamptonshire County Council onlinesafety@northamptonshire.gov.uk
- Twitter- https://twitter.com/NCCcybersafe
- Instagram - https://www.instagram.com/ncccybersafe/?hl=en

- https://www3.northamptonshire.gov.uk/councilservices/children-families-education/younghttps://www3.northamptonshire.gov.uk/councilservices/children-families-education/young-northants/staying-safe/Pages/bullying-online-safety.aspxnorthants/staying-safe/Pages/bullying-online-safety.aspx
- https://www.westnorthants.gov.uk/directory/local-offer/6451a5ba-1cee-4b86-992chttps://www.westnorthants.gov.uk/directory/local-offer/6451a5ba-1cee-4b86-992c-ee42b2ec72a3ee42b2ec72a3

Northamptonshire Safeguarding Children partnership:

- http://www.northamptonshirescb.org.uk/

Northamptonshire Police:

- https://www.northants.police.uk/ ○ https://www.northants.police.uk/advice/advice-and-information/caa/child-abuse/onlinehttps://www.northants.police.uk/advice/advice-and-information/caa/child-abuse/online-child-abuse/child-abuse/

In an emergency (a life is in danger or a crime is in progress) dial 999. For other non-urgent enquiries contact Northamptonshire Police via 101

National Links and Resources for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety ○ ChildLine: www.childline.org.uk ○ Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

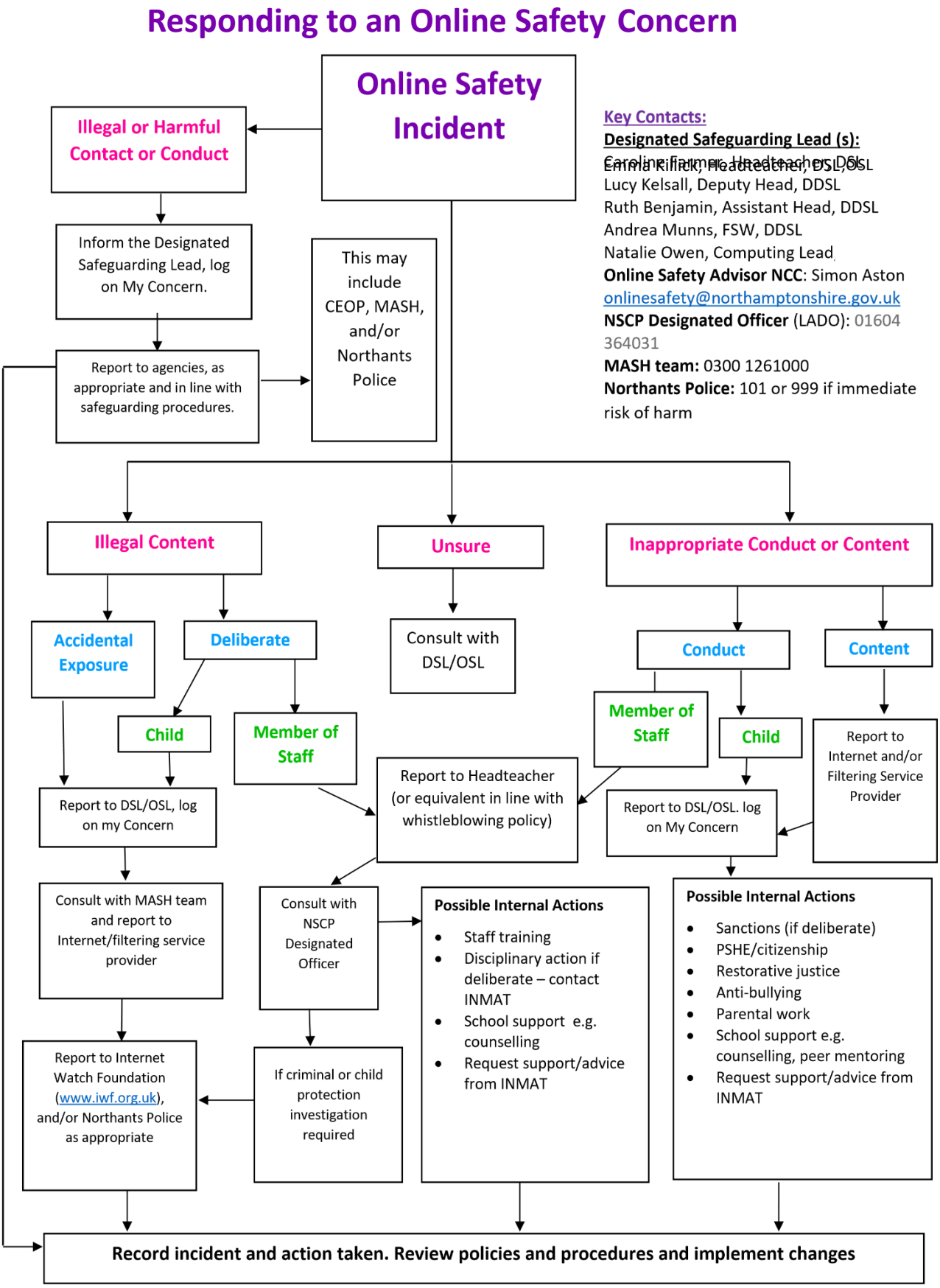
National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP: www.thinkuknow.co.uk www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety

- ChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

14. Appendices

Appendix 1



Appendix 2

The Abbey Primary School Online Safety Reporting Log

Reporting Log

Date	*Time*	*Incident (incl. name of pupil/s, year group)*	*Action Taken*		*Incident Reported By*	*Signature*
			What?	*By Whom?*		

Appendix 3


Childnet International
BE SMART ONLINE
S
SAFE
Keep your personal information safe. When chatting or posting online don't give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.
M
MEET
Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on www.thinkuknow.co.uk
THINK U KNOW
A
ACCEPTING
Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they've sent you.
R
RELIABLE
You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To find reliable information compare at least three different websites, check in books and talk to someone about what you have found.
T
TELL
Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – 0800 11 11 or www.childline.org.uk
BE SMART WITH A HEART
Remember to always be smart with a heart by being kind and respectful to others online. Make the internet a better place by helping your friends if they are worried or upset by anything that happens online.
WWW.CHILDNET.COM

Appendix 4

Pupil Rules for Responsible Internet Use

The school has laptops and tablets with Internet access to help our learning. These rules will keep everyone safe and help us to be fair and kind to others.

Rules 

- I will only use the tablets and laptops for schoolwork and homework
- I will ask permission from a member of staff before using the internet.
- I will only email using our school email address when my teacher has asked me to.
- The messages I send online will be polite and responsible.
- I will not share my personal details online, give my home address, telephone number or arrange to meet anyone under any circumstances.
- I will report any unpleasant material seen, or messages sent to me, to my teacher immediately.
- I understand that the school will check computer files and will monitor the internet sites that I visit.
- I will not access other people's files, passwords or impersonate others online.
- I will not bring in CDs, memory sticks or hard drives from outside school unless I have been given permission.
- I will not bring my mobile phone, device or smart watch into school.

Consequences 

- If I break the rules, it will result in a temporary or permanent independent ban on internet use or digital devices.
- A letter will be sent home or a meeting will be requested informing my parents of the incident.
- The Headteacher/Governing body of the school may decide to seek further actions if the rules are persistently broken.

Appendix 5 - Online harms and risks: curriculum coverage

Subject Area	Description and Teaching Content	Curriculum Area the Harm or Risk is Covered
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching will include the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm will be covered in the following curriculum areas: • Health education • Computing
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching will include the following: • What a digital footprint is, how it develops and how it can affect pupils' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Disinformation, misinformation and hoxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently Misinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g. releasing private information or photographs • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true	This risk or harm will be covered in the following curriculum areas: • Relationships and health education • Computing

Subject Area	Description and Teaching Content	Curriculum Area the Harm or Risk is Covered
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching will include the following: • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure • What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email • Who pupils should go to for support • The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following: • What identity fraud, scams and phishing are • That online fraud can be highly sophisticated and that anyone can be a victim • How to protect yourself and others against different types of online fraud • How to identify 'money mule' schemes and recruiters • The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal • The risk of sharing personal information that could be used by fraudsters • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details • How to report fraud, phishing attempts, suspicious websites and adverts	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing

Subject Area	Description and Teaching Content	Curriculum Area the Harm or Risk is Covered
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching will include the following: • Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching will include the following: • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How pupils can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching will include the following: • That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible to encourage them to spend money or generate advertising revenue • How notifications are used to pull users back online	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching will include the following: • How to find information about privacy settings on various sites, apps, devices and platforms • That privacy settings have limitations	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching will include the following: • How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing

Subject Area	Description and Teaching Content	Curriculum Area the Harm or Risk is Covered
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching will include the following: • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse • What acceptable and unacceptable online behaviours look like	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Radicalisation	Pupils are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals. Teaching will include the following: • How to recognise extremist behaviour and content online • Which actions could be identified as criminal activity • Techniques used for persuasion • How to access support from trusted individuals and organisations	All areas of the curriculum
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include the following: • What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal • How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why • That it is okay to say no and to not take part in a challenge • How and where to go for help • The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges	This risk or harm will be covered in the following curriculum areas: • Relationships education
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching will include the following: • That online content (sometimes gang related) can glamorise the possession of weapons and drugs • That to intentionally encourage or assist in an offence is also a criminal offence • How and where to get help if they are worried about involvement in violence	This risk or harm will be covered in the following curriculum areas: • Relationships education

Subject Area	Description and Teaching Content	Curriculum Area the Harm or Risk is Covered
Fake profiles	Not everyone online is who they say they are. Teaching will include the following: • That, in some cases, profiles may be people posing as someone they are not or may be 'bots' • How to look out for fake profiles	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, gangs and financial exploitation. Teaching will include the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	This risk or harm will be covered in the following curriculum areas: • Relationships education
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching will include the following: • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing

Subject Area	Description and Teaching Content	Curriculum Area the Harm or Risk is Covered
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching will include the following: • The issue of using image filters and digital enhancement • The role of social media influencers, including that they are paid to influence the behaviour of their followers • That 'easy money' lifestyles and offers may be too good to be true • The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm will be covered in the following curriculum areas: • Relationships and health education
Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching will include the following: • How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear or missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	This risk or harm will be covered in the following curriculum areas: • Health education
Online v's offline behaviours	People can often behave differently online to how they would act face to face. Teaching will include the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm will be covered in the following curriculum areas: • Relationships education
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching will include the following: • Strategies for positive use • How to build a professional online profile	This risk or harm will be covered in the following curriculum areas: • Relationships and health education
Suicide, self-harm and eating disorders	Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.	All areas of the curriculum