Online Safety Policy

Approved by:	TBC	**Date:** 1st October 2026
Last reviewed on:	October 2026	
Next review due by:	October 2027	

Contents

Introduction

Roles and Responsibilities

Skills awareness/development for all staff

Managing the school's online safety messages

Technical support

Digital Technology in the Curriculum

Remote Learning

Password Security

Data Security

Managing the Internet safely

Managing other Communication & Networking Technologies

Mobile Technologies

Managing email

Safe Use of Images / Video

Prevent Duty

Misuse and Infringements

Equal Opportunities

Parental Involvement

Writing and Reviewing this Policy

Appendices:

- Acceptable Use Agreement: Staff, Governors and Visitors
- Acceptable Use Agreement: Peripatetic teachers/coaches, supply teachers, student teachers
- Requirements for visitors, volunteers and parent/carer helpers
- Acceptable Use Agreement: Pupils – KS2
- Acceptable Use Agreement: Pupils – EYFS/KS1
- Headteacher's online safety letter to parents
- Acceptable Use Agreement: Parents
- Online safety policy guide for parents/carers
- Online Safety Reporting form (Staff)
- Online safety Reporting form (parents)
- Online safety Incident Log
- Online safety protocol Flowchart
- Guidance on responding to cyberbullying incidents
- Guidance on negative comments on social media

Introduction

We uphold the articles from the UN Convention on the Rights of the Child. These underpin this policy:

Article 17: Every child has the right to reliable information from the media. This should be information that they can understand. Governments must help protect children from materials that could harm them.

Article 19: Children have a right to be protected from all forms of harm.

Digital Technology in the 21st Century is seen as an essential resource to support learning and teaching, as well as in playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to equip our young people with the skills to access life-long learning and employment.

Whilst exciting and beneficial both in and out of the context of education, much of the digital technologies, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

This policy has been reviewed in response to recent legislation and the guidance outlined in the document:

Keeping Children Safe in Education - Sep 2025

Digital Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of these technologies within our society. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting (Audio Sharing)
- Video Sharing
- Music Sharing / Downloading
- Gaming
- Mobile / Smart phones with functionality including: text, video, web, audio, music, global positioning (GPS)
- Other mobile devices with similar functionality (tablets, laptops, gaming devices)

Ensuring children and young people are aware of the risks associated with the use of technologies, and can adopt safer behaviours, is vital in safeguarding them against cyber-bullying, sexting and grooming.

At Boxmoor, we understand the responsibility to educate our pupils on online safety issues teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

This policy relates to both fixed and mobile Internet technologies provided by the school, and technologies owned by pupils, parents and staff, but brought onto school premises.

Roles and Responsibilities

The Head teacher and Governors have ultimate responsibility to ensure that this policy and its practices are fulfilled and monitored. The Designated Safeguarding Lead has the additional role for ensuring the safety of children when they are working online at Boxmoor and will therefore also be recognised as the Online Safety Officer. The members of the safeguarding team and the IT Coordinator will provide support for the DSL with the associated responsibilities. All members of the school community will be made aware of the post-holder through Induction training, briefings and photographs on the Safeguarding board in the staffroom. It is the role of the Online Safety Officer to keep abreast of current issues and guidance through organisations such as Hertfordshire County Council, CEOP (Child Exploitation and Online Protection), UKCCIS (UK Council for Child Internet Safety), and Child net.

Senior Management and Governors are updated by the Head teacher/ Online Safety Officer and all Governors will be supported to gain an understanding of the issues and strategies at our school in relation to local and national guidelines, current legislation and advice.

This policy, supported by the school's Acceptable Use Agreements for staff, Governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Child Protection policy, Health and Safety, Home-School Agreement, Behaviour Policy, Anti-Bullying Policy and other curriculum policies.

Skills/awareness development for staff

Safeguarding and online safety is a responsibility of all members of staff and adults working with children. It is therefore paramount that staff are aware of the risks and issues relating to the online environment.

- Staff receive information and training on safeguarding and online safety through regular briefings and annual staff meetings.
- Details of the on-going local staff training programme are available through Hertfordshire County Council.
- New staff receive information on the school's Acceptable Use Agreement as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart in the appendices.)

- All staff are expected to incorporate activities and awareness in all areas where digital technologies are used.

Managing the school's online safety messages

- We endeavour to embed messages across the curriculum whenever the Internet and / or related technologies are used. This is particularly reinforced through IT lessons, PSHE sessions in relation to cyber-bullying and grooming, during assemblies and Safer Internet Days.
- The policy will be introduced to the pupils at the start of each school year.
- Posters will be prominently displayed in each classroom and in the library
- The school uses its internet and filtering provider's systems for security. These provide security for the school's computers as well as for individual users, and remind users of their obligations as a condition of logging in.

Technical support

The school has contracted an outsource company where the basic elements of online safety have been discussed and are regularly monitored and implemented.

Digital Technology in the Curriculum

Digital Technology and online resources are increasingly used across the curriculum. We believe it is essential for guidance to be given to the pupils on a regular and meaningful basis. Online safety is embedded within our curriculum and we continually look for new opportunities to promote it.

- Online safety lessons are delivered via the Teach Computing scheme of work.
- The school provides opportunities within a range of curriculum areas to teach online safety
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the curriculum.
- Pupils are aware of the relevant legislation when using the Internet such as data protection and intellectual property, which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respect for other people's information, images, etc through discussion, modelling and class activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum (Teach Computing)
- Regular assemblies, PSHE lessons or Safer Internet Days provide the opportunity to discuss issues relating to cyber-bullying and Internet grooming (e.g.: through respect for others and

appropriate / positive relationships). These lessons can equip pupils with the knowledge to use technology safely.

Remote Learning:

In the instance that we move to remote learning necessitated by a part/full school closure, the same principles of safeguarding, online safety and behaviour apply. In this event, we will endeavour to:

- Ensure consistency in the approach to remote learning for all pupils (Inc. SEND) who aren't in school through use of quality online/offline resources, teaching videos and virtual sessions
- Provide clear expectations to members of the school community with regards to delivery of high quality interactive remote learning
- Include continuous delivery of the school curriculum, as well as support of motivation, health, well-being and parent support
- Consider continued education for staff and parents (e.g. CPD, Supervision and Meet the Teacher)
- Support effective communication between the school and families and support attendance

The platform used will be the school's chosen online learning platform, which teachers will use to communicate with the children by posting learning materials to support independent learning at home.

Guidance for pupils:

The usual standard of behaviour expected during lessons in school still applies to any remote learning experience and sanctions/consequence will be applied, as necessary. Additional rules that pupils should follow are:

- be seated in an area that is conducive to learning (avoid the bedroom)
- Wear the school uniform (Years 1-6) and be appropriately dressed for the virtual lessons
- Start any lesson or meeting with their microphone muted and to only unmute when they are going to talk.
- Only use the chat function when asked by the teacher
- Encourage the pupil to speak to their parent and in turn their teacher, if anything makes them uncomfortable.

Guidance for staff

Staff are encouraged to carefully consider the opportunities and limitations presented by remote learning. The nature of working online, particularly where it involves 1:1 lessons, does pose

additional safeguarding and data protection challenges. Staff are advised to follow and observe these points for every remote lesson:

- Ensure the background is blurred or they are seated in a neutral area where nothing personal or inappropriate can be seen or heard in the background.
- Inform pupils that the lesson is to be recorded.
- Remind pupils of the expectations around behaviour and etiquette (e.g. they should start the lesson muted and unmute to ask questions). For 1:1 lessons, your line manager or a member of the SLT can always 'drop in' to lessons on occasion.
- When sharing their desktops with pupils as part of a lesson, it is advisable to only have open applications that will be used during the lesson.
- Any behavioural issues that occur during an online lesson should be dealt with as sensitively as would be the case in a physical lesson, and inform the SLT of any inappropriate repeated behavioural issues or safeguarding concerns.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, not even with their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's policy.
- Users are provided with an individual network and email log-in username. From Year 1 they are expected to use a personal password and are encouraged to keep it private.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If a user thinks their password may have been compromised or someone else has become aware of their password, they are expected to report this to the online safety officer.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and Arbor systems by ensuring that passwords are "strong"(a mix of upper and lower case letters, numbers and symbols), not shared and are changed periodically. Individual staff users must also make sure that workstations are not left logged on.
- Due consideration should be given by all users when logging into the browser/cache options (shared or private computer) which might retain usernames / passwords.

Managing the Internet

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and

vulnerable people. In our school access to the Internet is via the school's internet service provider. Internet is logged and the logs are randomly but regularly monitored upon request. Whenever any inappropriate use is detected, it will be followed up.

- At Boxmoor, students are supervised when accessing the Internet when working on laptops and chromebooks.
- Staff will preview any recommended sites before using it with students.
- Raw image searches (eg: Google image search) are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested. These will have been checked by the teacher. Where possible links from the school learning platform will be provided, it is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must always observe software copyright. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- The school's internet service provider provides, upon request, the facility to monitor and log web-based activity.
- School Internet access is controlled through our provider's effective web filtering service in line with the new legislation '*Keeping children safe in Education – September 2025*
- In addition, internet access is filtered for all users to ensure maximum protection from radicalisation materials when accessing the internet. Content lists are regularly updated and internet use is logged and regularly monitored. Request for filtering changes are logged by the online safety officer. Boxmoor is aware of its responsibility when monitoring staff communication under current legislation and considers the Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, and Human Rights Act 1998.
- Staff and pupils are aware that school-based email and Internet activity can be monitored and explored further if required.
- The school does not allow pupils access to Internet logs.
- If staff or pupils discover an unsuitable site, the screen must be switched off and the incident reported immediately to the online safety officer who will take the necessary steps to inform and report the url to the internet service provider.
- Anti-virus protection is installed on all school machines and is set to update automatically.
- In addition, any staff laptops used at home are also protected by the school's anti-virus software.
- Pupils and staff are not permitted to download programs or files on school equipment without seeking prior permission from the Head teacher and/or IT Coordinator.
- If there are any issues related to viruses or anti-virus software, the technical support company should be informed and this is communicated by staff through the IT support company's reporting system while also reporting the said issue to the online safety officer.

Managing other Communication & Networking technologies

The Internet includes a wide range of communication and networking tools & sites. Children need to be educated about appropriate ways of communicating and about the risks of making personal information too easily available. If used responsibly both outside and within an educational context, it can provide easy to use, creative, collaborative and free facilities.
However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

Social media is a broad term for any kind of online platform which enables people to directly interact with each other. Boxmoor denies access to social networking sites like Facebook, Pinterest, Twitter etc for all users within school. Although some video sharing websites like YouTube and Vimeo have elements of social media to them; when used safely and appropriately, it can offer numerous benefits and learning opportunities whilst supporting the many areas of the curriculum.

In order to prevent inappropriate images, bad language and unsuitable comments to be viewed by the children, staff have been advised of the following procedures:

- Searches, or first observations of a potential video, should not be carried out with any child in the classroom.
- Before showing the video to the class, the video should be watched and listened to carefully, for inappropriate content or material along with inappropriate comments that appear underneath the video, by the class teacher or TA,
- It is the class teacher's responsibility to make the final approval of a video.
- Teachers should also be aware of the advertisement on YouTube videos and these should be watched before showing the video to the children, without any children in the classroom.
- When showing the video to the children, ensure the board is frozen, stilled or muted prior to full screen mode being selected. Once the staff have finished watching their chosen video, it is imperative that the browser is closed so that the video sharing website cannot be accessed by children.
- Teachers are permitted to have YouTube channels if they are limited to appropriate educational content, and the ability for teachers and students to interact online is disabled.

In this way, children are made more aware of the need to use such sites safely when accessing them at home.

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites, which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, email address, specific hobbies/ interests).
- At the start of the academic year, pupils are advised to set and maintain profiles on such sites to maximise privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils are asked to report any incidents of cyberbullying to the Online Safety Officer.
- Pupils are introduced to a variety of Internet communication tools within the safe context of the school - learning platform.
- Staff understand that it is highly inappropriate to use social networking sites and other personal communication tools to communicate with pupils and / or parents (eg: Facebook, Twitter, email etc).
- Staff understand that it may considered a disciplinary offence if they mention issues concerning students / parents / carers / other staff associated with the school on social networking sites.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies (such as portable media players, tablets, gaming devices, Smart phones, etc) are familiar to children outside of school. Allowing such personal devices to access the school network can provide immense benefits in collaboration, but also create risks associated with misuse, inappropriate communications, etc. Emerging technologies will be examined for educational benefit and the risk assessed before such use of personal devices is facilitated in school. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to carry personal mobile phones whilst working, in order to support professional communication in relation to school matters. Phones will be on vibrate in the classroom and not used for personal reasons. In an emergency, the member of staff will seek permission from the DHT in advance or retrospectively, leaving the classroom to take the call.
- Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device unless directed to by the HT, dialling 141 beforehand.

- Pupils are allowed to bring personal mobile phones to school but must not use them on the school site. Phones should be turned off and given to the class teacher at the start of the school day; they will be locked away and it is the pupil's responsibility to ask for their phone back at the end of the day.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate messages between any members of the school community is not allowed.
- Permission must be sought before any image, video or sound recordings are made on these devices of any member of the school community.
- Capturing images & video on personal phones is not allowed by students / staff / parents unless on school equipment and for educational purposes.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (iPads)

- Where the school provides mobile technologies (cameras)) for offsite visits and trips, only these devices should be used to make image, video or sound recordings of any member of the school community.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and be aware of what constitutes good 'netiquette'. Children in KS2 are given an experience of sending and receiving email in their Online safety curriculum from Year 3 onwards.

Safe Use of Images / Video

Digital images / video are easy to capture, reproduce and publish and, therefore, easily misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images / video by staff and pupils with school equipment.
- Staff are not permitted to use personal devices, (eg: mobile phones and cameras), to record images of pupils; this includes when on field trips. However, with the express permission of the Head teacher, images can be taken; provided they are transferred immediately and
  solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal devices, (eg: mobile phones and cameras), to record images of the others, this includes when on field trips.

Consent of adults who work at the school

- Permission to use images / video of all staff who work at the school is sought on a regular basis and a copy is in the personnel file
- Parents are reminded, during assemblies and school performances, NOT to post images / video on social media.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos/ video in the following ways:

- on the school web site
- other printed publications that the school may produce
- recorded/ transmitted on a video or webcam
- in social media content created as a promotional material for the school
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg: divorce of parents, custody issues, etc.
Parents/ carers may withdraw permission, in writing, at any time.

- Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published.
- Only the Web Manager has authority to upload to the public website.

Storage of Images / Video

- Images/ video of children are stored on the school's network
- Pupils and staff are not permitted to use encrypted portable media (eg: USB storage devices) for storage of images however prior permission of the Headteacher is required if use is absolutely necessary.
- Right of access to this material is restricted to the teaching staff and pupils within the confines of the school network.
- The IT coordinator/technician has the responsibility of deleting the images when specified.

Webcams and CCTV

- CCTV is used in areas around the school site.

- The school uses CCTV for security and safety. Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school other than for special projects such as nature cams, which are streamed to the web.
- Webcams in school are only ever used for specific learning purposes. Images of children / adults are never broadcast.
- Webcams / CCTV is only used for staff training / development with the agreement / permission of the staff concerned
- Misuse of a webcam by any member of the school community will result in sanctions
    - All laptops in the school are equipped with a webcam.
    - Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils are supervised by a member of staff when video conferencing
- All pupils are supervised by a member of staff when video conferencing with end-points beyond the school.
- The school keeps a record of instances of video conferences, including date, time and participants.
- Approval from the Head teacher is sought prior to all video conferences within school.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be CRB checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.
- The school's Sexual & Relationships Education curriculum (SRE) provides a set of preventative tools which help safeguard pupils against cyber-bullying and grooming. The school has a comprehensive SRE policy in place which includes the appropriate teaching & learning of:
    a. Private and personal space
    b. Appropriate / safe and inappropriate / harmful relationships
    c. Consent

Prevent Duty

Boxmoor encourages children to show respect and tolerance towards different cultures, faiths and beliefs and to appreciate British values. We understand the importance of enabling our pupils to recognise and report unacceptable online behaviour.

Under the Counter Terrorism and Security Act 2015, Boxmoor has a statutory duty to have due regard to prevent children from displaying behaviour that can be attributed to extremism.

Any prejudice, discrimination or extremist behaviour, including derogatory language, displayed by pupils, staff or governors using digital technologies (web based or mobile) will always be challenged and where appropriate dealt with in line with our Online Safety Policy, Behaviour Policy for pupils, the Code of Conduct for staff and the Code of Conduct for governors.

Misuse and Infringements

Staff may lawfully search electronic devises, without consent or parental permission, if a pupil has a device not permitted in school or if staff suspect a device may be used to:

- Cause harm
- Disrupt teaching
- Cause personal injury
- Damage property

Any files, data or images that are believed to be inappropriate may be kept in evidence and passed to the relevant authorities.

Complaints

Complaints relating to online safety should be made to the Online Safety Officer or member of the Safeguarding team. Incidents may be logged by a member of the safeguarding team or IT Coordinator (see Incident Log in Appendix) and process should be followed (see Flowchart in Appendix). Parents use the quick link to CEOPS on the website to report any online safety incidents outside of school.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Online Safety Officer.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Online Safety Officer. Depending on the seriousness of the offence, this may lead to:
    - Involvement of a DSL and investigation
    - Reporting to CEOPS
    - Reporting to MASH
    - Reporting to the police
    - Immediate suspension
    - Dismissal

Equal Opportunities

Pupils with additional needs
The school endeavours to work in partnership with parents to convey a consistent message to all pupils. This in turn should aid the establishment and future development of the school's rules.

Staff are aware that some pupils will require additional reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of online safety. Activities are planned to make use of best available resources and are carefully managed for these children and young people.

Parental Involvement
At Boxmoor we believe that it is essential for parents/ carers to be fully involved with promoting online safety both in and outside of school while appreciating the benefits provided by technologies generally. We regularly consult and discuss with parents/ carers and seek to promote a wide understanding about the link between technology and safeguarding.

Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school policy through regular online safety awareness sessions and / or coffee mornings.

- Parents/ carers are asked to read through and sign Acceptable Use Agreements on behalf of their child on admission to school.
- Parents are expected to always be respectful in order to role model appropriate online behaviours and to be mindful of their own use of online technology.
- Parents/ carers are required to decide as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to online safety via:
    - Emails
    - Posters
    - Website
    - Newsletter items
    - Curriculum letters

Writing and Reviewing this Policy

Staff and pupil involvement in policy creation
Staff, Governors and pupils have been involved in making/ reviewing the policy through (school council, staff meetings, committee meetings).

Review Procedure
There will be an on-going opportunity for staff to discuss with the Online Safety Officer any issue of online safety that concerns them.

This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Safer Use Agreement / Computing Code of Conduct
Staff, Governors and Volunteers

The school Acceptable Use Agreement covers the use of all digital technologies in school (email, internet and intranet, network resources, learning platforms, software, equipment and systems). It is designed to ensure that all staff/governors/volunteers are aware of their responsibilities when using any form of digital technologies within their professional role. All members of the school community are expected to sign this agreement and always adhere to its contents.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Headteacher and Governing Body.
- I will not have my phone with me when working in the classroom, unless I have the permission of the DHT for a particular reason, otherwise my phone will be on silent in locked cupboard or locker.
- I will not reveal my password(s) or contact details to anyone.
- I will not allow unauthorised individuals to access email / Internet / network, or LA systems.
- I will not use the school server or school device to download or save sensitive or personal data onto a personal device.
- I will ensure that I work in a secure environment where my screen is not visible to others when working on sensitive or personal data.
- I will always log out when I finish working .
- I will report any data breaches to the SLT/ Data Protection Officer as soon as possible.
- I will not engage in any online activity that may compromise my professional responsibilities, including online searches.
- I will not attempt to use a personal system or personal login for remote teaching or set up any system on behalf of the school without SLT approval.
- I will not take secret recordings or screenshots of myself or pupils during live lessons.
- If teaching from home, I will conduct any video lessons in a professional environment**.** This means I will be correctly dressed and the camera view will not include any personal information or inappropriate objects , instead I will blur or change the background,.
- I am permitted to have YouTube channel to provide appropriate educational content to the students. I have disabled the ability for any student to interact and engage with the YouTube channel.
- I will only use the approved, secure email system(s) for any confidential school business.
- I will only use the approved school email or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business. I will not use my own phone to communicate with parents without prior approval of the Headteacher except in an emergency and I will withhold my number.
- I will not browse, download or send material that could be considered offensive.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the IT coordinator.
- I will undertake Cybersecurity training, keep abreast of the lastest advice to avoid scams and will not click on links in emails without checking the authenticity, download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive) that does not have up-to-date anti-virus software to the network / Internet and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras, tablets, laptops, smartwatches or other equipment for taking and transferring images of pupils or staff without permission. Any images stored will be for professional use only.
- I will not use a mobile phone, smartwatch or other photographing equipment of my own to take any pictures of children.
- I will ensure that I secure ICT hardware using appropriate safety measures:
    - My class laptop will always be secure.
    - Laptops/netbooks used by children will be locked away in the laptop/chromebook trolley at the end of each school day.

- Items of ICT hardware e.g. cameras, will be secured in lockable cupboards or desks when not in use.

- I will use cloud systems in accordance with School advice.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use".
- I will only use school hardware for business purposes, and personal purposes in a responsible way which minimises the risk of any data breaches. I understand that I will be subject to disciplinary procedures in line with our staff code of conduct and online safety policy, should any breaches occur.
- I will ensure any personal data is kept secure and confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me regarding staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's online safety curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to the Headteacher.

Within Social Networking:

- I will not contact pupils using social media or any other means not authorised by the school
- If any of my online activity affects students, staff or the wider community I understand that this could lead to disciplinary action
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I understand that I cannot publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- I will not use Social Networking sites for the promotion of personal financial interests, commercial ventures or personal campaigns
- I will not breach any of the school's policies.
- I will not discuss school events or matters, staff or pupils without prior permission from the Headteacher.
- I am aware that any negativity on WhatsApp may contravene the staff code of conduct and may be a disciplinary matter.
- I will not identify myself as a representative of the school.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date, read and understand the school's most recent online safety policies.

I agree to abide by all the points above.

I wish to have an email account and be able to use the school's ICT resources and systems.

I agree to follow this code of conduct and to support the safe use of Digital Technology throughout the school.

Full Name: _____(printed)

Role within the school: _____ Signature:__ Date:_____

Acceptable Use Agreement: Peripatetic teachers/coaches, supply teachers, student teachers*

**this agreement is applicable to student teachers not on the school staff*

School name: Boxmoor Primary School
Online safety lead: Dave Edwards
Designated Safeguarding Lead (DSL): Gareth Richards

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with the Headteacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the Headteacher or Deputy Headteacher.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, Headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with the Headteacher.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional

capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils. I will not 'friend' former pupils either; even where pupils have left the education system. You are reminded that young people can be considered as 'vulnerable' up until the age of 25. If you are concerned about this then you should consult with the Headteacher in the first instance.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information known as a result of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.
- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose or, in the case of 1:1 tuition, pupil's or parent/carer devices can be used, with parent/carer agreement.

Internet, mobile and digital technologies provide helpful recording functions but these cannot be made on a teacher's personal device. Recordings can be made with the child's and parent/carer's agreement on a school device, an organisational device approved by the Headteacher/DSL, or a young person's or parent/carer's own device.

Use of Email

I will use my professional or formal student email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

Use of personal devices

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Headteacher.

I will only use approved personal devices in designated areas and never in front of pupils. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support pupil learning. Pupils can also be encouraged, but not required, to access such apps on their own devices if allowed by the school and with parent/carer agreement.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of the Headteacher or Deputy Headteacher.

Promoting online safety

I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to the DSL or Deputy DSL.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the Headteacher or Deputy Headteacher.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature …… Date ……

Full Name …… (Please use block capitals)

Job Title/Role ……

Requirements for visitors, volunteers and parent/carer helpers

(Working directly with children or otherwise)

School name: Boxmoor Primary School
Online safety lead: Dave Edwards
DSL: Gareth Richards

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise any safeguarding concerns arising from your visit immediately with the Headteacher and/or DSL.

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.
- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.
- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils and parent/carers. Where appropriate I may share my professional contact details with parents/carers provided the DSL or Headteacher is informed before I leave the school.
- I understand my visit to the school may give me access to privileged information about pupils, staff, school systems and plans. Such information should never be shared online, including on social media sites.
- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the Headteacher.
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

Safer Use Agreement : Pupils – KS2

These rules will keep me safe and help me to be respectful towards others.

- I will only use the school's computers for schoolwork.
- I will keep my logins and passwords secret.
- If I bring a phone to school, I will switch it off and give it to my class teacher at the start of the day.
- I will think before I click! I will think before I search!
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will check the age restrictions when thinking about accessing a website or online game.
- I will be honest and not access games that are not for children my age.
- I will not talk about inappropriate computer games in school
- The messages I send will always be respectful, polite and sensible.
- I will only message or e-mail people I know, or a responsible adult has approved.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not use a AI specific website without the permission of my teacher or parent.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.
- I will take breaks, or agree device-free days with my parent.
- I will not have my own youtube account or post on social media to create my own online presence.
- I will not give in to peer pressure.
- I will use the Boxmoor or CEOPS website to report inappropriate online activity.

I have read and understand these rules and agree to them.

Name_____

Class_____

Signature _____Date _____

Safer Use Agreement: Pupils – KS1



I will only use the Internet when an adult is with me.



I can click on the buttons or links when I know what they do or my teacher has told me I can.



I will only send friendly messages to people I know.



If will only search for things an adult tells me is safe to search for. I see something I don't like on screen, I will tell an adult



I will keep my login and password secret.

Headteacher's online safety letter to parents: Early Years

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all children to be safe and responsible when using any IT. It is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read through these online safety rules with your child/ren and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you need to sign this agreement (on behalf of yourself and your child) to say that you agree to follow the rules. Any concerns or explanation can be discussed with the Headteacher, Mr Richards.

Please return the signed sections of this form which will be kept on record at the school.

Pupil agreement

Pupil name ……

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Parent signature (Early Years) on behalf of your child ……

Parent(s)/Carer(s) agreement

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child/ren. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or post material that may bring the school or any individual within it into disrepute.

(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents).

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.

Parent(s)/Carer(s) name(s) ……

Parent/carer signature ……

Date ……

Headteacher's online safety letter to parents: Key Stage 1 and Key Stage 2

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all children to be safe and responsible when using any IT. It is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read through these online safety rules with your child/ren and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you both need to sign this agreement to say that you agree to follow the rules. Any concerns or explanation can be discussed with the Headteacher, Mr Richards.

Please return the signed sections of this form which will be kept on record at the school.

Pupil agreement

Pupil name ……

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil signature (Key Stage 1 & 2 child) ……

Parent(s)/Carer(s) agreement

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child/ren. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or post material that may bring the school or any individual within it into disrepute.

(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents).

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.

Parent(s)/Carer(s) name(s) ……

Parent/carer signature ……

Date ……

Safer Use Agreement : Parents

Parent / carer name: _____Pupil name(s): _____

As the parent or legal guardian of the above pupil(s), I understand that my child may have access to IT devices, learn to use the Internet and other digital technology facilities at school.

- I understand that my child has signed a Safer Use Agreement.
- I understand that if my child brings a phone to school, it must be switched off and handed to the class teacher at the start of the day.
- I have read and discussed online safety rules with my child.
- I will promote the safe use of the Internet and digital technology at home.
- I will do my best to supervise, monitor and limit my child's use of devices.
- I will do my best to ensure my child does not access games or sites that are not age appropriate.
- I will not permit my child to have a WhatsApp group as I understand this often leads to problems between children.
- I will not allow my child to develop an online presence via youtube (13+) or social media sites.
- I will discourage my child from talking about inappropriate computer games in school.
- I will do my best to ensure that my child does not use AI specific sites to complete homework, unless directed to.
- I will make sure my child takes breaks from devices or arrange device-free days.
- I will do my best to ensure my child cannot access devices during the night so they get enough sleep.
- I will inform the school if I have any concerns over my child's online safety or use the school's website to report online safety issues to CEOPS.
- I understand that the school can check my child's computer files, my child's mobile and the Internet sites they visit and that if they have concerns about their online safety or online behaviour that they will contact me.
- I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, employing appropriate teaching practice and teaching online safety skills to pupils.
- I will role model appropriate use of the internet and consider my own behaviours when using WhatsApp, online technology and social media.
- I will role model appropriate use of cameras and phones in school and not record or film other members of the school community.
- I will not post images of children taken during class assemblies, performances or special events online.

Parent / carer Signature: _____Date: _____

Online safety policy guide for parents/carers: summary of key responsibilities

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for pupils.
- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.
- Parents/carers should not assume that pupils can bring technological devices to school and should always check the school policy.
- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.
- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.
- Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents/carers.

Please see the full online safety policy in the policies section on the school website.

Boxmoor Primary School

Online safety incident reporting form

Details of the person reporting the incident		
Name:	Phone number:	Email address:
Date of the incident:	Where did the incident take place?	
Description of the incident:		
Name(s) of those involved in the incident:	Age(s) of the child(ren) involved:	

Was the incident…(Please tick)				
Child on child ☐	Child on adult ☐	Adult on child ☐	Adult on adult ☐	Staff member on child ☐

Type of incident: (Please tick)					
Sexual ☐	Profanity ☐	Violence ☐	Bullying ☐	Grooming ☐	Other ☐
Please give details:					

How was the content accessed? (Please tick)						
School device ☐	Home tablet ☐	Mobile phone ☐	Email ☐	Internet browser ☐	Social media ☐	App ☐

School use
What action was taken with those involved in the incident?
What action was taken regarding the content accessed?

What follow up action was taken? (Please tick)		
Referral to LADO ☐	Referral to Children's services ☐	Advice to parents ☐

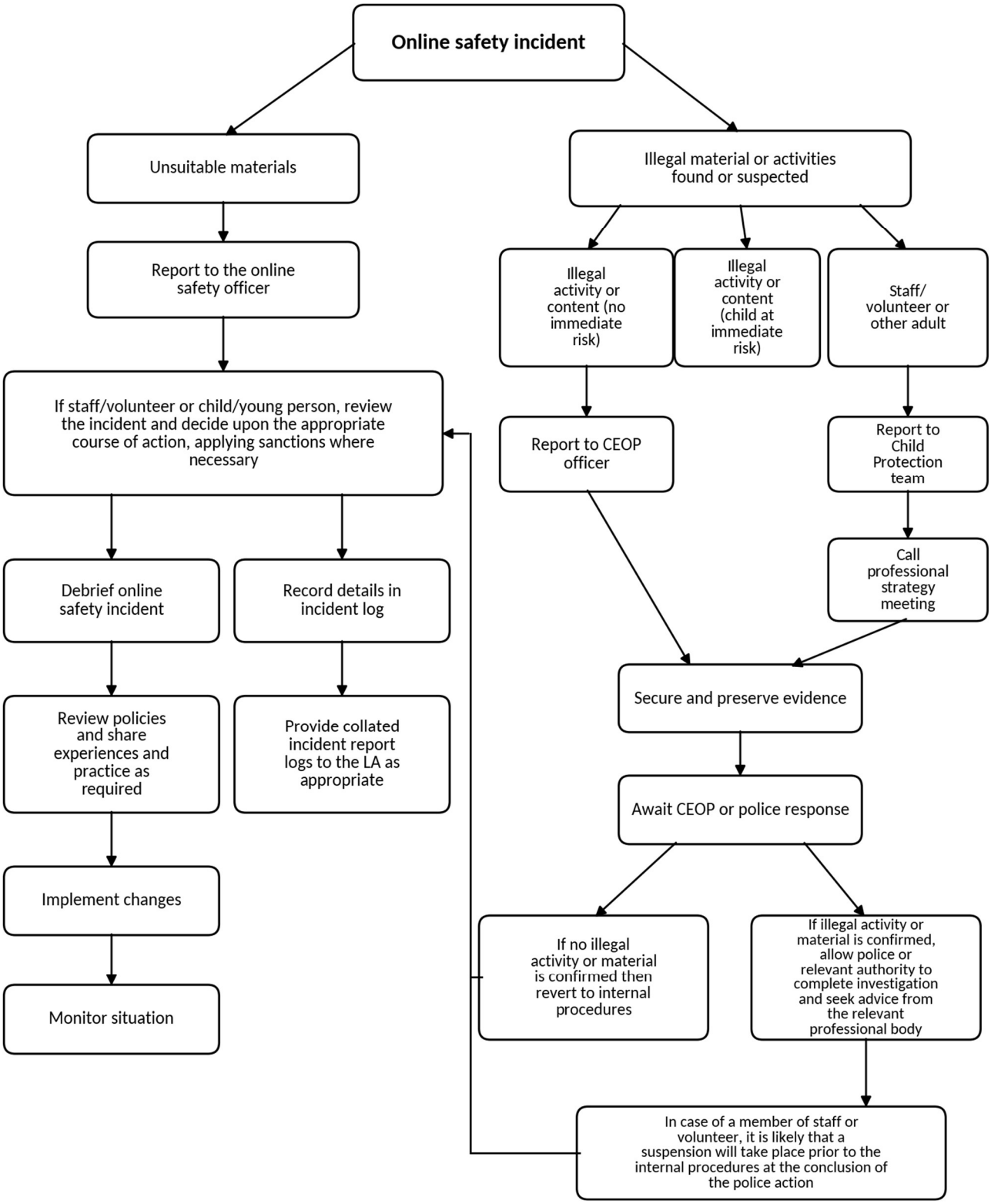
Police investigation □	Other □	
Please provide details:		

Online Safety **Incident Log – Boxmoor Primary School**

Details of ALL online safety incidents are to be reported to the Online Safety Coordinator. This incident log will be monitored by the Head teacher and shared with the governors.

Date and time	Name of pupil or member of staff	Device location/ number	Details of incident (including evidence)	Actions and next steps

Online safety **protocol Flowchart**



Guidance on responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, Headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the Headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Guidance for staff on preventing and responding to negative comments on social media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially the Online safety policy guide for parents/carers, clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

Collect the facts

As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the Headteacher will need to follow the school's safeguarding procedures.

If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

Addressing negative comments and complaints

Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

The meeting must:

- Draw attention to the seriousness and impact of the actions/postings;
- Ask for the offending remarks to be removed;
- Explore the complainant's grievance;
- Agree next steps;
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;
- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may

well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.