WOODMANSEY CE
PRIMARY SCHOOL

Woodmansey CE Primary School

E-Safety Policy (including Filtering and Monitoring and Acceptable Use)

Sep 2017, Reviewed Sep '19, Jan '22, **Sep '23**

1. OVERVIEW

This eSafety policy was created by M Britton and B Nicholls and the Senior Management Team at Woodmansey CE Primary School.
The policy was completed on: 29/09/2017
The policy was approved by the governing body in October 2017.

2. INTRODUCTION

At Woodmansey CE Primary School we fully recognise, acknowledge and embrace the importance and benefits of a 'connected' world. The opportunities for learning created by providing access to such a world are limitless and must therefore become part of day-to-day teaching and learning in school.

Being part of the internet community, as well as providing the aforementioned opportunities, also opens up the possibilities of exposure to dangers which would otherwise not be present, for example: access to inappropriate materials, contact with potentially dangerous strangers, 'cyber' bullying and identity theft. It must therefore be the role of the school to ensure that such risks are minimised, and, more importantly, that children are provided with the knowledge, skills and attitude necessary to become positive, safe and healthy on-line citizens.

3. RESPONSIBILITIES OF THE SCHOOL COMMUNITY

We believe that eSafety is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Management Team

• Develop and promote an eSafety culture within the school community.
• Support the eSafety coordinator in their work.
• Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to eSafety effectively.

- Receive and regularly review eSafety incident logs and be aware of the procedure to be followed should an eSafety incident occur in school.
- Take ultimate responsibility for the eSafety of the school community.

Responsibilities of the eSafety Coordinator

- Promote an awareness and commitment to eSafety throughout the school.
- Be the first point of contact in school on all eSafety matters.
- Lead the school eSafety group.
- Create and maintain eSafety policies and procedures.
- Develop an understanding of current eSafety issues, guidance and appropriate legislation.
- Ensure all members of staff receive an appropriate level of training in eSafety issues
- Ensure that eSafety education is embedded across the curriculum.
- Ensure that eSafety is promoted to parents and carers.
- Liaise with the local authority, the local safeguarding children's board and other relevant agencies as appropriate.
- Monitor and report on eSafety issues to the SMT as appropriate

Responsibilities of the Designated Safeguarding Lead

- To liaise with the e-safety coordinator and leadership team on all issues regarding online safety
- To ensure that e-safety issues are logged and dealt with appropriately and further action is taken when necessary
- To liaise with external agencies when appropriate
- To regularly review filtering and monitoring to ensure procedures are being followed and filtering is adequate
- To follow up reported incidents of access to inappropriate material online as appropriate.
- Ensure an eSafety incident log is kept up-to-date using CPOMs.

Responsibilities of Teachers and Support Staff

- Read, understand and help promote the school's eSafety policies and guidance.
- Read, understand and adhere to the school staff AUP.
- Develop and maintain an awareness of current eSafety issues and guidance.
- Model safe and responsible behaviours in your own use of technology.

- Embed eSafety messages in learning activities where appropriate.
- Supervise pupils carefully when engaged in learning activities involving technology.
- Be aware of what to do if an eSafety incident occurs.
- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Pupils

- Help and support the school in creating eSafety policies and practices; and adhere to any policies and practices the school creates.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.
- Take responsibility for your own and each other's 'safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by pupils outside of school.
- Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home.
- Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know of someone who this is happening to.
- Discuss eSafety issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

- Help and support your school in promoting eSafety.
- Read, understand and promote the school pupil AUP with your children.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies that your children use in school and at home.
- take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Discuss eSafety concerns with your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in your own use of technology.
- Consult with the school if you have any concerns about your children's use of technology.

Responsibilities of Governing Body

• Read, understand, contribute to and help promote the school's eSafety policies and guidance.
• Develop an overview of the benefits and risks of the Internet and common technologies used by pupils.
• Develop an overview of how the school ICT infrastructure provides safe access to the Internet.
• Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
• Support the work of the eSafety leader in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafety activities.
• Ensure appropriate funding and resources are available for the school to implement their eSafety strategy.

4. TEACHING AND LEARNING

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our pupils 'lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the Internet brings.

• We will provide a series of specific eSafety-related lessons in every year group/specific year groups as part of the ICT curriculum / Jigsaw PSCHE curriculum / other lessons.
• We will celebrate and promote eSafety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
• We will discuss, remind or raise relevant eSafety messages with pupils routinely wherever suitable opportunities arise during all lessons; including **the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.**
• Staff will model safe and responsible behaviour in their own use of technology during lessons.

5. HOW PARENTS/CARERS ARE INVOLVED

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:

- hold an annual parent meeting on eSafety / include eSafety as part of an annual parent meeting
- include useful links and advice on eSafety regularly in newsletters / on our school website
- include a section on eSafety in the School handbook

6. MANAGAING IT SYSTEMS AND ACCESS

The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.

- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware and will be kept active and up-to-date.
- The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.
- Internet access will be supervised AT ALL TIMES by a member of staff. This applies also when children are using **iPads** to access the internet.
- Members of staff will abide by the school AUP at all times.
- Any administrator or master passwords for school ICT systems should be kept secure and available to at least two members of staff, e.g. head teacher and member of technical support.
- The wireless network in school is encrypted to reduce the risk of unauthorised access.
- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur.
- The school will regularly audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate.

We will regularly review our Internet access provision, and review new methods to identify, assess and minimize risks.

7. FILTERING AND MONITORING

- The school uses a filtered Internet service. The filtering is provided through Smoothwall.
- The DSL has lead responsibility for overseeing all filtering and monitoring concerns and reports.
- Filtering and monitoring procedures will be reviewed annually by the DSL and any adjustments made where necessary.
- Filtering will be checked regularly using the SWGFL tool here: https://swgfl.org.uk/services/test-filtering/
- Smoothwall monitoring will provide daily logs of inappropriate content that has been searched for or attempted website visits. This logs the time, IP address and search term or web address.
- As appropriate, these logs will be followed up by the DSL. This might mean a general reminder to a class or group, chasing up any particular concerns that staff might have with particular children. It might be necessary to look at search history in particular class / year group if there is a more serious concern.
- Staff will receive annual update training on filtering and monitoring procedures.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the DSL. The incident should be logged using CPOMs under 'Cause for Concern' / 'Internet Content Concern'
- When necessary, parents will be informed if children have accessed inappropriate content.
- If users discover a website with potentially illegal content, this should be reported immediately to the DSL. The school will report this to appropriate agencies including the filtering provider, LA or CEOP.

8 LEARNING TECHNOLOGIES IN SCHOOL

	Pupils	Staff
Personal mobile phones brought into school	Yes (in Y6 with parental consent)	Yes
Mobile phones used in lessons	No	Not if avoidable
Mobile phones used outside of lessons	No	Yes
Taking photographs or videos on personal equipment	No	Yes Photos to be downloaded to school laptop ASAP to increase security.
Taking photographs or videos on school devices	Yes	Yes
Use of hand-held devices such as PDAs, MP3 players or personal gaming consoles	No (unless permitted as gem treat which must still follow guidance in this policy)	Yes
Use of personal email addresses in school	No	Yes
Use of school email address for personal correspondence	No	No
Use of online chat rooms	No	No
Use of instant messaging services	No	Yes
Use of blogs, wikis, podcasts or social networking sites	Yes – as controlled by filtering	Yes – as controlled by filtering
Use of video conferencing / online video meetings	Supervised	Yes

9 USING EMAIL

- Pupils should use approved e-mail accounts allocated to them by the school, and be aware that their use of the school e-mail system will be monitored and checked.
- Staff should use their school e-mail address for correspondence relating to school.
- Foundation and Y1,2,3,4 classes will be allocated an individual e-mail account for use by pupils within that class, under supervision of the class teacher.
- Pupils will be reminded when using e-mail about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mail from an unknown sender, or viewing/opening attachments.
- Pupils are not permitted to access personal e-mail accounts during school.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.

Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.

10 USING IMAGES, VIDEO AND SOUND

- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
-
- Digital images, video and sound will be created using equipment provided by the school, or equipment owned by staff who have signed the agreement in the staff AUP, that images of children will not be kept on personally owned computer equipment.
- Staff and pupils will follow the school policy on creating, using and storing digital resources.
- In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff/pupils involved.
- If pupils are involved, relevant parental permission will also be sought before resources are published online.

11 USING BLOGS, WIKIS, PODCASTS, SOCIAL NETWORK AND OTHER WAYS FOR PUPILS TO PUBLISH CONTENT ONLINE

We use blog /social media (eg Twitter and Facebook) /other ways to publish content online to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner.
Blogging, podcasting and other publishing of online content by pupils will take place within the areas the school has provided for such material. These will include: the school website, school blogs, Instagram, Twitter, YouTube, Showbie.
Pupils will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them. Pupils will not use their real name when creating such resources. They will be encouraged to create an appropriate 'nickname'.
Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside of school.

12 USING VIDEO CONFERENCING AND OTHER ONLINE VIDEO MEETINGS

In the future we might use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. However, we will ensure that staff and pupils take part in these opportunities in a safe and responsible manner.

- All video conferencing activity will be supervised by a suitable member of staff.
- Pupils will not operate video conferencing equipment, or answer calls, without permission from the supervising member of staff.
- Video conferencing equipment will be switched off and secured when not in use / online meeting rooms will be closed and logged off when not in use.
- Pupils will be given appropriate user rights when taking part in an online meeting room. They will not have host rights or the ability to create meeting rooms.
- Video conferencing should not take place off school premises without the permission of the head teacher.
- Parental permission will be sought before taking part in video conferences.

- Permission will be sought from all participants before a video conference is recorded. Video conferences should only be recorded where there is a valid educational purpose for reviewing the recording. Such recordings will not be made available outside of the school.

13 USING MOBILE PHONES

• Pupils' personal mobile phones are not allowed in school unless parental permission has been given when children are in Y6.
• Pupils will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up such that only those features required for the activity will be enabled.
• Use of staff mobile phones for school purposes will be refunded if necessary. Staff would prefer to carry and use their own mobile phones on school visits, rather than a 'school mobile'. Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent.

14 USING NEW TECHNOLOGIES

• As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an eSafety point of view.
• We will regularly amend the eSafety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an eSafety risk.

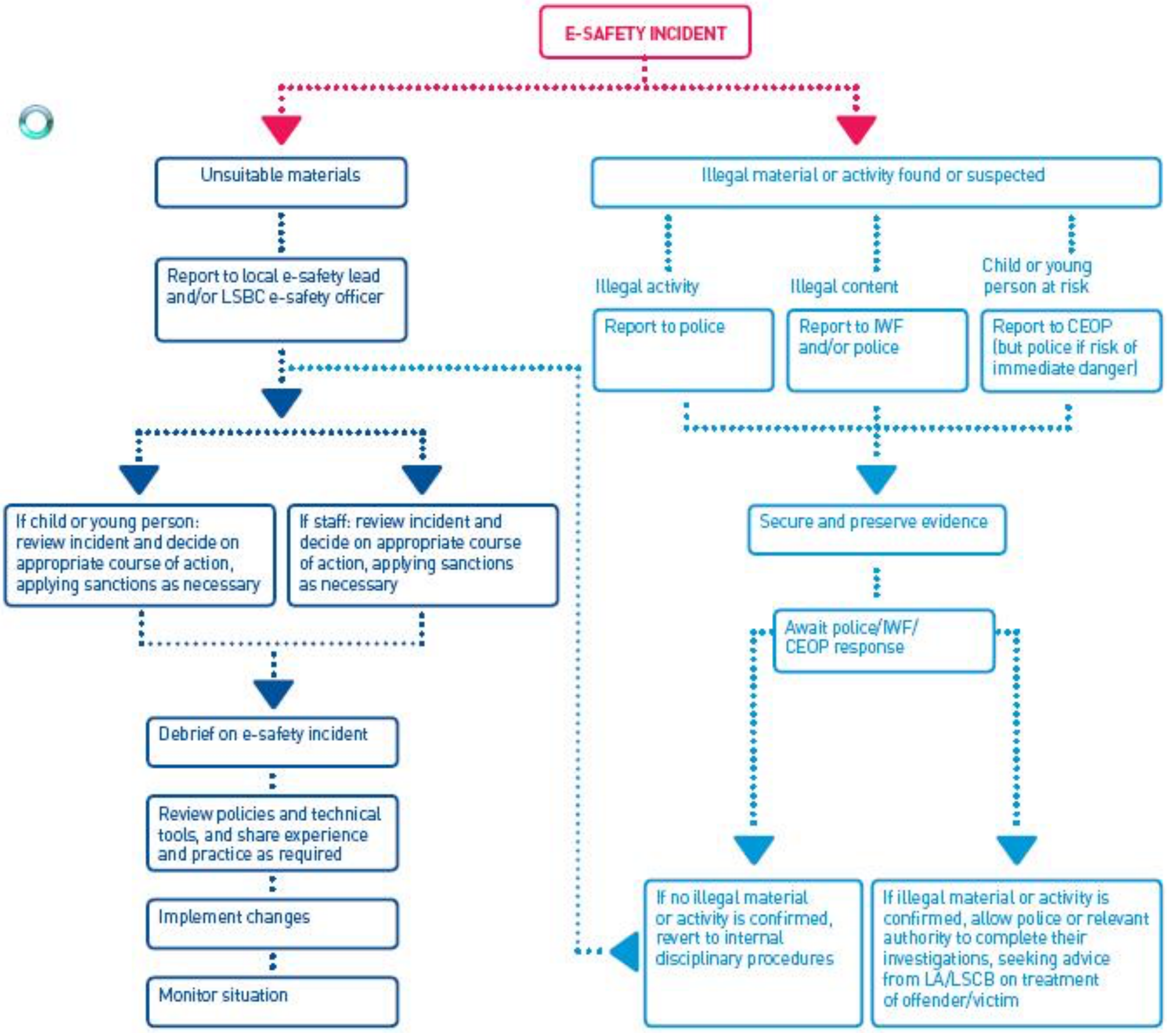
15 PROTECTING PERSONAL DATA

• We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998 and the EU initiated GDPR legislation (see policy).
• Staff will ensure they properly log-off from a computer terminal after accessing personal data.
• Staff will not remove personal or sensitive data from the school premises without permission of the headteacher. Any data which is impractical to ensure is kept in school (eg Reports) will be kept secure, by use of school laptops which are password protected and password protecting individual documents which contain pupil data.

16 SCHOOL WEBSITE AND OTHER ONLINE CONTENT PUBLISHED BY THE SCHOOL

- The school website will not include the personal details, including individual e-mail addresses or full names, of staff or pupils.
- A generic contact e-mail address will be used for all enquiries received through the school website.
- All content included on the school website will be approved by the head of school before publication.
- The content of the website will be composed in such a way that individual pupils cannot be clearly identified.
- Staff and pupils should not post school-related content on any external website without seeking permission first.

DEALING WITH E-SAFETY INCIDENTS


E-SAFETY INCIDENT
Unsuitable materials
Illegal material or activity found or suspected
Report to local e-safety lead and/or LSBC e-safety officer
Illegal activity
Illegal content
Child or young person at risk
Report to police
Report to IWF and/or police
Report to CEOP (but police if risk of immediate danger)
If child or young person: review incident and decide on appropriate course of action, applying sanctions as necessary
If staff: review incident and decide on appropriate course of action, applying sanctions as necessary
Secure and preserve evidence
Await police/IWF/ CEOP response
Debrief on e-safety incident
Review policies and technical tools, and share experience and practice as required
Implement changes
Monitor situation
If no illegal material or activity is confirmed, revert to internal disciplinary procedures
If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from LA/LSCB on treatment of offender/victim

Woodmansey CE Primary School – Staff Acceptable Use Policy

These statements are designed to ensure staff and other adults in school are aware of their professional responsibilities when using the ICT systems provided. All staff should follow the guidelines at all times. You are responsible for your behaviour and actions when accessing the Internet at school, whether on your own or school equipment, and when using school ICT equipment at other locations such as your home.

- Any use of school ICT systems will be for professional purposes as agreed by the school senior management team

- Usernames, passwords and other logon details should be kept secure and not revealed to anyone else. Care should be taken to ensure you logout when not actively using the ICT systems. You should not allow an unauthorised person to access the school ICT systems, e.g by logging in for them.

- Any online activity should not harass, harm, offend or insult other users.

- You will not search for, download, upload or forward any content that is illegal, or that could be considered offensive by another user. If you accidentally encounter such material you should follow your school's procedure and report this immediately.

- You should not download or install any hardware or software without permission. If you have responsibility for installing software you should be confident it is adequately licensed and appropriate for educational use.

- Ensure that any files on removable media (e.g. USB drives, CDs) are free from viruses and other malware before use and that such devices are not used for carrying sensitive data or details of pupils, parents or other users without suitable security and without permission from the Head teacher.

- Any electronic communications with pupils or parents should be related to schoolwork only, and should be through school e-mail addresses or other school systems e.g. learning platforms. **It is not acceptable to contact pupils (or ex-pupils who are under 18) using personal equipment or personal contact details, including your own mobile phone or through your personal social network profiles.**

- Any online activity, including messages sent and posts made on websites, and including activity outside of school, should not bring your professional role or the name of the school into disrepute.

- Any still or video images of pupils and staff should be for professional purposes only. They should be stored, transferred to and used on school equipment. Such images should not be stored on personally owned devices.

- You will not give out your personal details, or the personal details of other users, to pupils or parents or on the Internet. In particular you should ensure your home address, personal telephone numbers and email accounts are not shared with children, young people or parents.

- You should ensure that any personal or sensitive information you use or access (e.g. SIMS data, assessment data) is kept secure and used appropriately. **All files which contain data about children must be password protected.**

- Personal or sensitive information should only be taken off-site if agreed with the head teacher, and steps should be taken to ensure such data is secure. Your notebook and iPad must have a password protected login.

- You should respect intellectual property and ownership of online resources you use in your professional context, and acknowledge such sources if used.

- You should support and promote the school e-Safety Policy, and promote and model safe and responsible behaviour in pupils when using ICT to support learning and teaching

- You understand that your files, communications and Internet activity may be monitored and checked at all times to protect your own and others 'safety, and action may be taken if deemed necessary to safeguard yourself or others. If you do not follow all statements in this AUP and in other school policies, you may be subject to disciplinary action in line with the school's established disciplinary procedures.

Signed………………………………………………………………

Name (Printed) ……………………………………………………