Wootton St Andrew's Church of England (VA) Primary School

January 2025

Online Safeguarding Policy (E-Safeguarding)

Our Vision for Online Safety

Technology is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. We recognise that the school needs to build on the use of these technologies in order to equip young people with the appropriate skills to access life-long learning and employment.

Teaching and learning involves accessing a wide range of resources including web-based resources and mobile technology. It is also important to recognise the constant and fast paced evolution of technology within our society as a whole. The main online technologies children and young people are using include:

- Websites and apps
- Email, instant messaging, text and chat
- Social networking
- Photo and video sharing
- Digital media consumption
- Digital media creation
- Online Gaming
- Mobile devices
- Games consoles and other devices with an internet connection e.g. smart TV
- Learning platforms and Virtual Learning Environments

At Wootton St Andrew's Primary School we are proactive in educating our pupils about 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 classroom environment. We believe it is essential for online safety guidance to be given to the pupils on a regular and meaningful basis. Online safety is embedded within our curriculum, practices and online presence, and we continually look for new opportunities to promote online safety.

Our vision is that pupils have a diverse, balanced and relevant approach to the use of technology, in an environment where security is balanced appropriately with the need to learn effectively. We aim to ensure that our children are equipped with the skills and knowledge to use technology appropriately and responsibly, that they understand the risks associated with this activity and are able to deal with these both in and out of school.

As part of online safety education, we will teach children:

- How to use technology safely, responsibly, respectfully and securely
- Where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- What positive, healthy and respectful online relationships look like
- The effects of their online actions on others
- How to recognise and display respectful behaviour online

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- How to identify online risks
- The risks of sharing personal information and how to keep their personal information private
- Why age restrictions exist and why they are important
- What a digital footprint is, how it develops and how it can affect them in the future

Wootton St Andrew's online safety policy has been developed to ensure safety measures are in place to protect both students and staff working with computing equipment and related technologies. The policy will assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own and students' standards and practice. Our responsibility is to set high expectations of our students using communication technologies and to maintain a consistent approach to online safety.

To demonstrate our commitment to online safety, the school is working towards the 360 Degree Safe accreditation, which shows that our policies, practices and infrastructure meet a rigorous standard.

Scope of Policy

- This policy applies to the whole school community including Wootton St Andrew's senior leadership team, school board of governors, all staff employed directly or indirectly by the school, visitors, students and pupils.
- Wootton St Andrew's senior leadership team and school board of governors will ensure that any relevant or new legislation that may impact upon the provision of online safety within school will be reflected within this policy.
- The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students or pupils when they are off the school site. This is pertinent to incidents of cyber bullying, or other online safety related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
- The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate online safety behaviour that takes place out of school.
- This policy should be read alongside the staff and pupil acceptable use policies, the technical security policy, social media policy and behaviour policy.

Review and Ownership

This online safety policy:

- Has been developed by the school E-safeguarding leaders together with the Computing subject leader and safeguarding leaders, and is current and appropriate for its intended audience and purpose.
- Has been endorsed and agreed by the senior leadership team and approved by governors.
- Will be reviewed annually or when any significant changes occur with regards to the technologies in use within the school.
- The school has appointed a member of the governing body to take lead responsibility for online safety.

Our Shared Responsibility

Schools (and registered childcare providers) in England and Wales are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" (Revised Prevent Duty Guidance: for England and Wales).

Furthermore, it expects that schools "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology". The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school IT system." However, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

We believe that online safety is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for teaching and learning.

The following list of responsibilities shows how each member of the community will contribute to the school vision.

1. The Senior Leadership Team

- The head teacher is ultimately responsible for safeguarding provision (including online safety) for all members of the school community, with day-to-day responsibility for online safety delegated to the E-safeguarding leaders.
- The senior leadership team will ensure that appropriate technical safeguards (filtering and monitoring) are in place on the school's internet connection and that all school devices are properly managed to ensure that children are protected from access to harmful material online whether this be extremist, terrorist or inappropriate in nature.
- The head teacher and senior leadership team will ensure that the E-safeguarding leaders and other relevant staff receive effective and up to date training to enable them to carry out their E-safeguarding roles and to train other colleagues when necessary.
- The senior leadership team will receive routine updates from the E-safeguarding leaders as appropriate.
- The head teacher and senior leadership team will ensure that procedures are rigorously followed in the event of all online safety incidents.
- The head teacher and senior leadership team will receive timely, regular and routine updates and reports on all online safety incidents.
- The team will ensure that online safety education is appropriately embedded across the whole curriculum.

2. The E-Safeguarding Leaders

- Will promote an awareness and commitment to online safety throughout the school.
- To be the first point of contact in school on all online safety matters.
- Take day-to-day responsibility for online safety within school and to have a leading role in establishing and reviewing the school online safety policies and procedures.
- Have regular contact with other online safety committees.
- Will communicate regularly with the designated online safety governor and the senior leadership team.

- Will create and maintain online safety policies and procedures, reporting to governors at least annually.
- Will ensure that online safety is promoted to parents and carers.
- Monitor and report on online safety issues to the senior leadership team as appropriate.
- Understand the issues surrounding the sharing of personal or sensitive information.

3. Teachers and Support Staff

Are required to:

- Read, understand and actively promote the school's online safety policy and associated policies and guidance.
- Read, understand, sign and adhere to the school Staff and Governor's Acceptable Use Agreement.
- Ensure that any online safety incidents are reported under appropriate escalation routes.
- Develop and maintain an awareness of current online safety issues and guidance.
- Model safe and responsible behaviours in their own use of technology.
- Ensure that any digital communications with pupils should be on a professional level and only through approved systems, never through personal mechanisms, e.g. personal email, text, mobile phones or personal social networking accounts etc.
- Embed online safety messages in learning activities across all areas of the curriculum.
- Supervise and guide pupils carefully when engaged in learning activities involving technology.
- Ensure that pupils are fully aware of safe and critical research skills and methods.
- Be aware of online safety issues related to the use of mobile phones, cameras and other internet connected devices.
- Understand and be aware of incident reporting mechanisms that exist within the school.
- Maintain a professional level of conduct in personal use of technology at all times.

4. Contracted IT Support Providers

Are required to:

- Ensure the senior leadership team are given appropriate advice and information regarding technical aspects of the school's online safety strategy.
- Be aware of the school's online safety policies and guidance.
- Read, understand and adhere to the school Staff and Governor's Acceptable Use agreement.
- Report any online safety related issues that come to their attention to the E-safeguarding leaders.
- Develop and maintain an awareness of current online safety issues, legislation and guidance relevant to their work.
- Maintain a professional level of conduct in the use of technology at all times.
- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Ensure that pupil access to the school network is only through an authorised, restricted mechanism.

5. Pupils

Are required to:

- Understand, sign and adhere to the Pupil Acceptable Use Agreement (students who are unable to understand the acceptable use agreement may require a parent/ guardian to sign on their behalf).
- Help and support the school in the creation of online safety policies and practices and to adhere to any policies and practices the school creates.
- Where appropriate pupils will be expected to understand and abide by school policies on the use of mobile phones, digital cameras and other devices.
- Know and understand school rules relating to bullying and cyberbullying.
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- Understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and to understand the incident-reporting mechanisms that exist within school.
- Discuss online safety issues with family and friends in an open and honest way.

6. Parents and Carers

Are asked to:

- Help and support the school in promoting online safety.
- Read, understand and promote the school pupil's acceptable use agreement with their children.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies that their 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 online safety concerns with their 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 their own use of technology.
- Consult with the school if they have any concerns about their children's use of technology.
- Sign the photography permission form upon admission stating where photographs are to be published.
- Sign a GDPR agreement.

7. Governors

Have agreed to:

- Read, understand, contribute to and help promote the school's online safety policies and guidance.
- Read, understand, sign and adhere to the Staff and Governor's Acceptable Use Agreement.
- Nominate one governor to have specific responsibility for online safety.
- Develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- Develop an overview of how the school's IT infrastructure provides safe access to the internet by receiving regular reports at governor meetings.

- 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 safeguarding committee and E-safeguarding leads in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in online safety activities.
- Make funds available to provide for the safe use of technology for pupils and adults within the school.

8. Designated Safeguarding Leader

Has a specific responsibility to:

- Understand the dangers regarding access to inappropriate online contact with adults and strangers.
- Liaise regularly with the E-safeguarding leaders.
- Be aware of potential or actual incidents involving grooming of young children.
- Be aware of and understand cyber bullying and the use of social media for this purpose.
- Be aware of the risks posed by 'sexting'.
- Be aware of their responsibilities in regard to safeguarding children from extremist and terrorist material online.

9. Other External Groups

- The school will liaise with local organisations to establish a common approach to online safety and the safe use of technologies.
- The school will be sensitive and show empathy to internet-related issues experienced by pupils out of school and offer advice where appropriate.
- The school will provide an acceptable use agreement for any guest who needs to access the school computer system or internet on school grounds (e.g. parent helpers, trainee teachers, work experience pupils).

10. Managing Digital Content

- Before photographs of pupils can be published, permission must be granted formally and agreed and signed by parents or guardians. All staff should be aware of the process involved with publishing images over different mechanisms.
- Parents and carers may withdraw permission, in writing, at any time. A procedure exists for permission to be removed retrospectively.
- The school will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Pupils and staff will use only school equipment to create digital images, video and sound. In particular, digital images, video and sound will not be taken without the written permission of the person with parental responsibility; 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 other than on the school website, app or school-approved social networking accounts in accordance with permissions.

- Parents may take photographs at school events; however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including on social networking.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

11. Storage of Images

- Any images, videos or sound clips of pupils must be stored on school devices and never transferred to personally-owned equipment.

12. 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 recognise that three main areas of online safety risk are:

1. Content – Children and our communities need to be taught that not all content is appropriate or from a reliable source.
2. Contact – Children and stakeholders need to be made aware that digital technologies may be used as a vehicle for grooming, cyber bullying and identity theft, and understand how to deal with these risks if they occur.
3. Conduct – Children and parents need to be aware that their personal behaviour online and their electronic identity can increase the likelihood of, or cause harm to themselves and others. Key risk areas being disclosure of personal information, issues around sexting, privacy issues and copyright issues.

In order to minimise these risks to our pupils at Wootton St Andrew's:

- We will ensure that the internet connection coming into school will be filtered for inappropriate, illegal, extremist and terrorist content and all devices available to children will be centrally managed to ensure appropriate technical safeguards are in place.
- We will discuss, remind or raise relevant online safety 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.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- Pupils will be taught about the impact of bullying and cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

- Pupils will be made aware that some means of communication through technology are inappropriate and can be dangerous or illegal e.g. 'sexting', exploitation, communicating with unknown people through social media, trolling.
- We will provide regular online safety information to parents and carers.

13. Staff Training and Awareness

- Our staff will receive regular information and training on online safety issues in the form of regular and routine updates and when appropriate.
- As part of the induction process, all new staff will receive information and guidance on the online safety policy and the school's acceptable use agreements.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff will be encouraged to incorporate online safety activities and awareness within their curriculum areas.
- Staff will be trained on any new systems, software and practices.
- The school will be responsible for ensuring that access to computers, networks and the internet 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.
- Members of staff will access the network using an individual username and password, which they will keep secure.
- Users should log out after each session and not allow other adults or pupils to access the network through their username and password.
- Users will abide by the school acceptable use agreements at all times.
- Staff will return all equipment and media at their exit interviews.

13a Parent/Carer and Community Awareness

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

- Newsletters, the website, the Parentmail app
- Parents/carers sessions
- High profile events e.g. Safer Internet Day
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Sharing our online safety expertise and good practice

14. Passwords and Security

- A secure and robust username and password convention exists for all system access.
- Staff are prompted to change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.
- Staff should change their passwords whenever there is any indication of possible system or password compromise.
- Pupil passwords will be managed by the appropriate member of support/teaching staff and changed when is deemed appropriate.
- All pupils have individual accounts for accessing Chrome devices and online learning platforms.
- All pupil devices will be centrally managed to ensure technical safety features are tuned on and kept on.
- All staff have a responsibility for the security of their username and password. Staff must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Laptops leaving the site will be encrypted as an additional layer of security.
- When off site, staff will log into their laptop via a secure remote connection.

15. 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 online safety point of view. We will regularly amend the online safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an online safety risk.

- The school will audit computer equipment usage to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- Methods to identify, assess and minimise risks will be reviewed regularly.

16. Mobile Phones

- Any pupil who brings his or her mobile phone or personally-owned device into school should switch it off and hand it into staff.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised to contact the school reception if the need arises.

17. Staff Use of Mobile Devices

- Staff are permitted to use their own mobile phones or devices for contacting parents when outside of the setting in a professional capacity (eg. on a school trip).
- Staff will use a school phone to contact parents or carers when in the setting.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use provided school equipment for this purpose.
- If a member of staff breaches the school policy, then disciplinary action may be taken.

18. Filtering Internet Access

The school filters and monitors its internet provision appropriate to the age and maturity of pupils to ensure the risk of accessing harmful content is minimised.

- The school will provide an appropriate content filter is in place to filter out any extremist, terrorist or inappropriate material on the incoming internet connection and that this is applied to all devices on the school network. The filter will ensure illegal content is blocked by: employing the Internet Watch Foundation (IWF) blacklist to block access to illegal Child Sexual Abuse Material (CSAM); Integrating 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'.
- Filtering will apply to all devices accessing the internet via the school's internet connection. This includes Windows laptops, Google Chromebook and Apple iPads and Android tablets.
- A different level of filtering can be delivered to users of Microsoft Windows devices (staff) to ensure staff have access to services and content needed to perform their roles (eg YouTube on staff devices).
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision, by adding to our own blacklists/whitelists as appropriate.
- The school will have a clearly defined procedure for reporting breaches of filtering.
- All staff and pupils will be aware of this procedure by reading and signing the acceptable use agreement and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the E-Safeguarding Leads. All incidents will be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the E-safeguarding Leads. The school will report such incidents to appropriate agencies including the filtering provider, the local authority or CEOP.
- The school will regularly review the filtering product for its effectiveness.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.
- Pupils will be taught to assess content as their internet usage skills develop.
- Pupils will use age-appropriate tools to research online content.
- The evaluation of online content is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Additional Technical Safeguards

In addition to content filtering, additional technical safeguards will be in place:

- All traffic into and out of the school will pass through a firewall
- All pupil devices will be centrally managed to ensure any available safety features are enabled and that pupils are unable to circumvent these safety features.
- Web browsers on pupil and staff devices will be centrally managed to ensure 'safe search' is enabled and cannot be disabled.
- The school wi-fi network will be password protected
- Operating systems and software on all devices will be patched with the latest security updates supported on that device.
- Anti-virus software will be installed, enabled and automatically updated on all supported devices.

19. Internet Access Authorisations

- Parents will be asked to read the school acceptable use agreement for pupil access and discuss it with their children, when and where it is deemed appropriate.
- All pupils will have the appropriate awareness training through online safety lessons and, where possible, sign the pupil acceptable use agreement prior to being granted internet access within school.
- All staff will be offered online safety training, which will be updated annually, and sign the staff acceptable use agreement prior to being granted internet access within school.
- Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.
- The school will maintain a current record of all staff and pupils who have been granted access to the school's internet provision.
- Any visitor who requires internet access will be asked to read and sign an acceptable use agreement.
- All pupils will be closely supervised and monitored during their use of the internet.
- Pupils will be frequently reminded of internet safety issues and safe usage.

20a. Email and Online Communication

Staff are required to comply with the following:

- Staff should only use approved email accounts allocated to them by the school and should be aware that use of the school email system is monitored and checked.
- Staff should not use personal email accounts on any school devices or during directed times.
- Access, in school, to external personal email accounts may be blocked.
- The school gives all staff their own email account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Staff are responsible for keeping their password secure.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Irrespective of how staff access their school email (from home or within school), school policies still apply.
- Staff should check email accounts regularly for new correspondence.
- Staff should never open attachments from an untrusted source.
- 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 email system or receipt of any inappropriate messages from another user should be reported to a member of the E-safeguarding Team.
- Any unsolicited inappropriate emails should be reported to the E-safeguarding Leads in addition to being reported as spam via the email client before being deleted.

Gmail is not enabled for pupils. Teachers and pupils can communicate via other approved web-based platforms (eg Activelearn).

Pupils are expected to:

- Use secure, school-provided accounts within school.

- Immediately tell a designated member of staff, teacher or trusted adult if they receive any inappropriate or offensive messages.
- Send only polite and responsible messages.
- Learn to keep personal information confidential within online conversations.
- Learn to not reveal personal details of themselves or others in online communications.
- Learn to never arrange to meet with anyone following an online conversation.
- Use the school-provided accounts to develop safe and respectful practices.

20b. Video Conferencing

Google Meet is included within Google Classroom should this be required to provide remote learning to pupils. Staff may also use other approved video conferencing services such as Zoom or Microsoft Teams as part of their professional roles.

Staff and pupils must ensure the safe use of video conferencing.

Staff will:

- Meet professional standards for dress and conduct
- Ensure only class teachers set up Google meetings (unless permission has been given)
- Use their school accounts to set up meetings
- Share the Google meeting link only on Google Classroom
- Continue to follow school policies, including the Safeguarding and Child Protection Policy
- End the meeting if the safety of the staff member or children is compromised and immediately report any concern to the head teacher.

Pupils will:

- Try where possible, to use Google Meet in a central area of the house
- Follow the school expectations for behaviour
- Ensure anything said or shared is appropriate
- Not share the meeting ID with anyone else
- Dress appropriately Parents should:
- Try where possible, to ensure their child is in a central room in the house
- Try where possible, to ensure that other members of the household understand that a Google meeting is taking place and that they should not appear in the background of the call
- Try where possible, to ensure that the background is neutral and does not contain any personal information
- Not record any part of the Google meeting
- Not share any sensitive information another child may say during these calls

21. Using Blogs and Other Mechanisms to Publish Content Online

- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Any public blogs run by staff on behalf of the school will be hosted on the learning platform, school website, app or other school-approved service and postings should be approved by the head teacher before publishing.
- Teachers will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform, website, app or school social

networking account. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them.

- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, networking sites and other online publishing outside school.

22. Use of Social Media (See Social Media Policy)

23. Electronic Bullying and harassment (See also the Anti-Bullying Policy)

This online safety policy recognises the additional dangers of cyberbullying. All staff and pupils should be aware that any misuse of technology to bully or harass others will be dealt with under the school Anti Bullying Policy, and are reminded that:

'Bullying is behaviour by an individual or group, repeated over time, which intentionally hurts another individual or a group physically or emotionally. Bullying can take many forms (for instance, cyber-bullying via text messages or the internet), and is often motivated by prejudice against particular groups (for example on grounds of race, religion, gender, sexual orientation, or because a child is adopted or has caring responsibilities). It might be motivated by actual differences between children, or perceived differences. Stopping violence and ensuring immediate physical safety is obviously a first priority but emotional bullying can be more damaging than physical. All staff will have to make their own judgements about each specific case.'

24. Management of Assets

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant IT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

25. Special Requirements

When appropriate and deemed essential, the school will seek to ensure that all users have access to computing equipment and related services through the use of specially adapted hardware and software systems.

26. Dealing with and Reporting Incidents

All online safety incidents at Wootton St Andrew's are logged and recorded, with procedures regularly audited by the E-safeguarding Team.

Staff need to be aware of the following issues:

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the head who will refer this to appropriate external authorities such as the police, CEOP, Internet Watch Foundation or other agencies as appropriate.
Examples of illegal offences that should be reported to the police include:

- child sexual abuse images and content

- adult material which potentially breaches the Obscene Publications Act Inciting racial hatred
- criminally racist material
- incidents of ‘grooming’ behaviour
- the sending of obscene materials to a child
- offences under the Computer Misuse Act
- Terrorist and extremist material

Other activities e.g. cyber-bullying could also lead to criminal prosecution.

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. The computer in question should be isolated as any change to its state may hinder a later police investigation.

Staff should never under any circumstances investigate, interfere or share evidence of child sexual abuse as they may themselves be committing an illegal offence in doing so. Further information is available from www.iwf.org.uk.

Inappropriate Use

Staff and pupils at Wootton St Andrew’s Primary School are likely to have to deal with ‘accidental’ access to inappropriate materials and content. Examples of these and the actions and sanctions to apply are as follows:

1. Accidental access to inappropriate content. Recommendation is to minimise the application, turning off the device, closing the laptop etc. Pupils should tell a trusted adult. Staff will enter the details on the incident log, and advise the E-safeguarding leads to notify the filtering and monitoring company.
2. Using other people’s logins, accounts or passwords.
3. Deliberate searching for inappropriate materials.
4. Bringing unauthorised electronic media into school.
5. Inappropriate use of email, chat and forums.

Recommendation for each of the above is to inform the E-safeguarding leads, who will enter the details onto the incident log, re-iterate and raise online safety issues with the individual or class, and for more serious or persistent offences consider disciplinary action and parent/guardian involvement.

Wootton St Andrew’s Primary School has a well-developed system of sanctions and rewards. Pupils work as a class team to earn reward time each week as a reward for good behaviour, with loss of break or lunch time constituting a sanction for inappropriate behaviour (see Relationships & Behaviour Policy for details).

In addition to these general sanctions, where there has been a breach of acceptable use, pupils may also have their account suspended, and lose any other internet privileges (such as using computers at play or free choice time), for one week.

Approved by:	Headteacher:	R.Zaitschenko	Date Approved:	January 2025
	Chair of Governors:	Rev.A.Wright	Review Date:	January 2026
	Governors:	K.Hewson, A.Morgan		