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

January 2024

E-Safeguarding

Aims of the Policy

- To set out the key principles expected of all members of the school community at Wootton St Andrew's VA C of E Primary School (WSA) with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff of WSA Primary School.
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To minimise the risk of misplaced or malicious allegations made against adults who work with pupils.
- This policy applies to the whole school community including the senior leadership team, governors, all staff employed directly or indirectly by the school and all pupils.
- The senior leadership team and school board of governors will ensure that any relevant or new legislation that may impact upon the provision for E:Safeguarding 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 and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. Linked to our aim to uphold the Christian values of trust and family, this is pertinent to incidents of cyberbullying, or other E:Safeguarding-related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
- To ensure that the school follows GDPR guidance for safe storage of personal and sensitive information.
- 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 E:Safeguarding behaviour that takes place out of school.

Review of the policy

- The school teaching staff will be responsible for document ownership, review and updates of this policy with the support of the senior leadership team.
- The school E:Safeguarding policy has been agreed by the staff and approved by governors.
- The E:Safeguarding policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school and the wider community.
- All amendments to the school E:Safeguarding policy will be discussed with all members of school staff.

Communication of the policy requirements

- The senior leadership team will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school E:Safeguarding policy and the use of any new technology within school.
- The E:Safeguarding policy will be provided to and discussed with all members of staff.
- All amendments will be shared with all members of the school community. This will be via the school website and via email.
- The contents of the policy will be discussed by the school council/school buddies to ensure the language and vocabulary is appropriate and understandable for the policy's intended audience.
- An E:Safety module will be included in the PSHE, Citizenship and Computing curriculums covering key details of the school policy.
- An E:Safeguarding training programme will be established across the school to include a regular review of the E:Safeguarding policy.
- Pertinent points from the school E:Safeguarding policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within school.
- The key messages contained within the E:Safeguarding policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed E:Safeguarding messages across the curriculum whenever the internet or related technologies are used.
- The E:Safeguarding policy will be introduced to the pupils at the start of each school year.
- E:Safeguarding posters will be prominently displayed around the school.

Roles and responsibilities

Responsibilities of the senior leadership team

- The head teacher is ultimately responsible for E:Safeguarding provision for all members of the school community, though the day-to-day responsibility for E:Safeguarding will be delegated to the Computing and Technology subject leader, PSHCE leader, learning mentor, anti-bullying co-ordinator and the appointed governor with responsibility for Computing and E:Safeguarding.
- The head teacher and senior leadership team are responsible for ensuring that the relevant staff receive suitable training to enable them to carry out their E:Safeguarding roles and to train other colleagues when necessary.
- The head teacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious E:Safeguarding incident.
- The head teacher and senior leadership team should receive update reports from the Computing and Technology subject leader, PSHCE leader, learning mentor and anti-bullying co-ordinator termly or in the event of a serious E:Safeguarding incident.

Responsibilities of the E:Safeguarding team (Computing and Technology subject leader, PSHCE leader, learning mentor, anti-bullying co-ordinator and appointed governor.)

- To promote an awareness and commitment to E:Safeguarding throughout the school.
- To be the first point of contact in school on all E:Safeguarding matters.
- To take day-to-day responsibility for E:Safeguarding within school and to have a leading role in establishing and reviewing the school E:Safeguarding policies and procedures.
- The school will use the **360 degree safe** self-review online tool specifically for schools. This is to ensure the school meets Government expectations and constantly reviewing practises to meet needs.
- To have regular contact with other E:Safeguarding committees, e.g. the local authority, Local Safeguarding Children Board, YHGFL and CEOP.
- To communicate regularly with the senior leadership team.
- To create and maintain E:Safeguarding policies and procedures.
- To develop an understanding of current E:Safeguarding issues, guidance and appropriate legislation.
- To ensure that all members of staff receive an appropriate level of training in E:Safeguarding issues.
- To ensure that E:Safeguarding education is embedded across the curriculum.
- To ensure that E:Safeguarding is promoted to parents and carers.

- To monitor and report on E:Safeguarding issues to the senior leadership team as appropriate.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an E:Safeguarding incident.

Management and use of digital content

- Written permission from parents or carers will be obtained at the beginning of each school year.
- Parents and carers may withdraw permission, in writing, at any time.
- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound.
- We 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 only use school equipment to create digital images, video and sound. In exceptional circumstances, personal equipment may be used with permission from the head teacher provided that any media is transferred solely to a school device and deleted from any personal devices. 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 and pupils involved.
- If pupils are involved, relevant parental permission will also be sought before resources are published online.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Storage of images

- All staff must follow GDPR guidance of storage of personal information using encryption codes.
- Any images, videos or sound clips of pupils must be stored on the school devices and never transferred to personally-owned equipment.
- Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.
- The Computing and Technology subject leader has the responsibility of deleting the images when they are no longer required, or when a pupil has left the school.

Learning and teaching

We will provide a series of specific E:Safeguarding-related lessons in every year group as part of the Computing and Technology curriculum and PSHCE curriculum.

- We will provide lessons on how to keep their GDPR safe relating to internet safety.
- We will celebrate and promote E:Safeguarding through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant E:Safeguarding 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.
- We will remind pupils about their responsibilities through an Internet Safety Policy which will be signed each year.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- All pupils will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of 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 Child line or the CEOP report abuse button.

Staff training

- Our staff will receive regular information and training on Safeguarding issues in the form of staff meetings and online courses.

- As part of the induction process all new staff receive information and guidance on the E:Safeguarding policy and the school's Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of E:Safeguarding 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 E:Safeguarding activities and awareness within their curriculum areas.

Managing ICT systems and access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- All access to school ICT systems should be based upon a 'least privilege' approach.
- 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.
- All users will sign an Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.
- At Key Stage 1 all internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times.
- At Key Stage 2, pupils will have increased independent access with supervision.
- Members of staff will abide by the school AUP at all times.

Passwords

- All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords.
- All staff must follow GDPR guidance on protecting access.
- All access to school information assets will be controlled via username and password.
- Access to personal data is securely controlled in line with GDPR.

Emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in school is allowed.
- All new technologies will be tested and reviewed for any security vulnerabilities that may exist. Suitable countermeasures will be adopted within school to ensure that any risks are managed to an acceptable level.
- Emerging technologies can incorporate software and/or hardware products.
- The school will periodically review which technologies are available within school for any security vulnerabilities that may have been discovered since deployment.
- All new technologies deployed within school will be documented within the E:Safeguarding and Acceptable Use Policies prior to any use by any member of staff or pupil.
- The acceptable use of any new or emerging technologies in use within school will be reflected within the school E:Safeguarding and Acceptable Use policies.
- Prior to deploying any new technologies within school, staff and pupils will have appropriate awareness training regarding safe usage and any associated risks.
- The school will audit ICT equipment usage to establish if the E:Safeguarding policy is adequate and that the implementation of the E:Safeguarding 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.

Filtering internet access

- The school uses a filtered internet service. The filtering system is part of the schools' broadband agreement and managed by Adept/ACS technical support and Rob Adams.
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- 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 Policy 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 team. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the E:Safeguarding team. The school will report such

incidents to appropriate agencies including the filtering provider, the local authority and 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 internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Internet access authorisations

- All parents will be required to sign the home-school agreement prior to their children being granted internet access within school.
- Parents will be asked to read the school Acceptable Use Policy for pupil access and discuss it with their children, when and where it is deemed appropriate.
- All pupils will have the appropriate awareness training and sign the pupil Internet Safety Policy prior to being granted internet access within school.
- All staff will have the appropriate awareness training and sign the staff Acceptable Use Policy 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.
- Any visitor who requires internet access will be asked to read and sign the Bring Your Own Device policy.
- When considering internet access for vulnerable members of the school community the school will make decisions based on local knowledge.
- Key Stage 1 pupils' internet access will be directly supervised by a responsible adult.
- Key Stage 2 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.

Email

- Staff should only use approved email accounts allocated to them by the school whilst using school systems and should be aware that any use of the school email system will be monitored and checked.
- 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.

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. A full audit trail can be made available should this become necessary.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

Mobile phone usage in schools

General issues

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times. (8.45am -12 1pm-3.45pm and during staff meetings/INSET).
- Mobile phones and personally owned devices may only be used in the staff room or offices and not in classrooms, corridors, toilets and playground.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- In line with previous statements, no images or videos should be taken on mobile phones or personally-owned mobile devices (See Storage of Images).

Pupils' use of personal devices

- No pupil should bring his or her mobile phone or personally-owned device into school. Any device that has to be brought into school for safety reasons must be handed into the office at the start of the school day and will be returned at 3.30pm.
- The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices brought into school that are not handed into the office.
- If a pupil is found to have a mobile phone or mobile devices that have not been handed to the office, these devices will be confiscated and returned only to a parent/carer.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity. If there are to be exceptions to this i.e. school visit, SATS invigilation, emergencies, permission must first be sought from the head teacher.
- Where staff members have to use a mobile phone for school duties in an emergency they should use their own devices and hide (by inputting 141) their own mobile numbers for confidentiality purposes.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and

mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personal device as part of an educational activity then it will only take place when approved by the senior leadership team.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Data protection and information security

- The school community will act and carry out its duty of care for the information assets it holds in line with its Data Protection Act 1998 commitments.
- The school will ensure it meets the GDPR guidance for accessing and storing personal information of staff and pupils using appropriate access/ passwords and storage devices.
- The storage devices of personal information to be evaluated and recorded.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The school has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within school.
- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
- All computers that are used to access sensitive information should be locked (Ctrl-Atl-Del) when unattended.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.
- Fax machines will be situated within controlled areas of the school.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All personal and sensitive information taken offsite will be secured through appropriate technical controls, e.g. encrypted memory stick.

- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

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 ICT equipment will be disposed of through an authorised agency.
- School equipment for teachers to be stored securely overnight so that is not on display.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

Approved by:	Headteacher	R.Zaitschenko	Date Approved:	January 2024
	Chair of Governors:	Rev.A.Wright	Review Date:	January 2025
	Governors:	K.Hewson, A.Morgan		