Woodley Church of England (Controlled) Primary School

Whole School ICT Policy

Responsibility of:	Teaching and Learning Committee
Type of Policy:	School Policy
Reviewed:	Tri-Annually
Date of Review:	September 2023

Chair of Governors:

Head Teacher:

Whole School ICT Policy and Procedures

Roles and Responsibilities

Governors

The Governor in our school responsible for the effectiveness of this policy is Peter Fahy.
The Governing Body

- Have regular meetings with the school e-Safety Co-ordinator, **C. Blakely**.
- Regular monitor e-safety incident logs completed on a school E-Safety form which are stored securely
- Report to relevant sub committees.
- Keep up to date with school e-Safety matters.

Head Teachers and SMT

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of our school community. The day-to-day responsibility for e-safety has been delegated to the ICT Co-ordinator, **C. Blakely** or another appropriate member of staff.
- The Headteacher /SMT are responsible for ensuring that such staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues when necessary. The Senior Management Team will receive regular monitoring reports.
- The Headteacher and the ICT Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher and School Business Manager ensure that the Information Commissioner's Office, ICO, registration is kept up to date on an annual basis.

e-Safety Co-ordinator

- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place through annual training.
- Ensures training and advice is provided for staff.
- Liaises with the Local Authority.
- Liaises with school ICT technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-Safety developments.
- Meets regularly with the ICT Strategy team (which includes Governors) to discuss current issues.
- Ensures the Headteacher is regularly reported to regarding e-safety.

PSHE Coordinator/curriculum coordinator

- PSHE Co-ordinator provides materials and advice for integrating e-safety within PSHE schemes of work. Our current PSHE Co-ordinator is **Joanne Daniell**.
- Checks that e-safety is taught on a regular basis.

The ICT Co-Ordinator, working with other school colleagues, is responsible for ensuring that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- the school meets the e-Safety technical requirements outlined in any relevant Local Authority e-Safety Policy and guidance
- Users may only access the school's networks through a properly enforced password protection policy.
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

- he/she keeps up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant
- the use of the network, learning platform and pupil email is regularly monitored in order that any misuse/attempted misuse can be reported to the ICT Co-ordinator for investigation and action.
- appropriate steps are taken to protect personal information, which may include the encryption of removable devices including laptops and external storage devices, and the provision of secure access to the school network from home where necessary using VPN or equivalent technologies (installed on school equipment only). Refer to School Data Protection Policy for further information regarding data and how the school uses and protects it.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that

- They are familiar with current e-safety matters and of the school e-safety policy and practices.
- They have read, understood, signed and work to the school Staff Acceptable Use Policy (AUP). (**Appendix A**)
- They report any suspected misuse or problems to the ICT Co-Ordinator for investigation and action.
- Digital communications with learners (email/Virtual Learning Environment (VLE)/voice) should be on a professional level and only carried out using approved school systems.
- E Safety is taught to all ages throughout each term, through a mapped two-year cycle. E-safety issues are embedded in all aspects of the curriculum and other school activities.
- Learners understand and follow the school e-safety and pupil acceptable use policy. (**Appendix Bi-v**)
- Learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations in relation to their age.
- They monitor ICT activity in lessons, extracurricular and extended school activities.
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that they are aware of the procedure for dealing with any unsuitable material that is found in internet searches.

Child Protection Officer (CPO) – Designated Safeguarding lead

The DSL, **Mrs Louisa Gurney**, should be trained in e-safety issues and be aware of child protection matters that may arise from

- Sharing or loss of personal data. – **refer to Data Protection Policy**
- Access to illegal/inappropriate materials.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

Data Protection Officer

Responsible for maintaining registration with the Information Commissioner's Office, keeping abreast of regulatory requirements and recommendations as outlined on their website at www.ico.gov.uk and informing staff and leadership so that school policies may be updated. Refer to school Data Protection Policy. The School Data Protection Officer is **Mrs Caroline Thomas.**

e-Safety within learning and teaching

- Key e-safety messages are reinforced as part of a planned programme of assemblies, PSHE activities or other curriculum opportunities where appropriate.
- Learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.

- Learners should be helped to understand the need for the AUP (Acceptable Use Policy) and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of computers are displayed in all rooms and displayed next to fixed site computers.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.
- Staff will be kept up to date through regular training in e-Safety.

Network Security

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented by those responsible.
All staff have an individual password which complies with the school password procedures below. Pupils may have a group password or older pupils may be given individual passwords for accessing the network.

- All users have an individual log on to the learning platform.
- Servers, and communications cabinets should be securely located and physical access restricted.
- Wireless systems are secured to at least WPA level (Wi-Fi protected access)
- All users will have clearly defined access rights to school ICT systems.
- The “administrator” passwords for the school ICT system, used by the ICT Co-Ordinator are also available to all members of the SLT and stored securely in school.
- The school maintains and supports the managed filtering service provided by SEGfL.
- Changes to network filtering should be approved by the ICT Co-Ordinator.
- Any filtering issues are to be reported immediately to the ICT Co-Ordinator and SEGfL.
- School ICT technical staff may monitor and record the activity of all users from the school. Users are made aware of this through the Acceptable Use Policy.

School password protocol

- All passwords used by adults should follow the guidelines in this policy.
- No individual should log on using another individual’s password, unless they are a member of staff logging on as a child.
- No individual should tell another individual their password.
- Once a computer has been used, users must remember to log off so that others cannot access their information. Users leaving a computer temporarily should lock the screen.
- If you know your password is insecure then it is essential that the password is changed immediately.

Loading software

- Only the ICT Co-Ordinator or those acting specifically on his/her behalf are allowed to load software on to any school computer.
- For the purpose of this policy, software relates to all programs, images or screensavers, which can be downloaded or installed from other media.
- The only exceptions to this are teacher laptops, where individuals may download software if they are sure the rules below apply.
- Images and video clips may be downloaded as long as the teacher in charge is satisfied that they are not breaching copyright.

- Software loaded on to any school system must be
    - Properly licensed.
    - Free from viruses.
    - Authorised by the ICT Co-ordinator.

Virus Protection

- All computer systems, including teacher laptops, must be protected by an Antivirus product which is administered centrally and automatically updated.

The Technician uses a range of security software to remove adware and malware.

Special Categories of Personal data

The definition of Special Categories of Personal Data is any data which links a child's name to particular item of information.

Thus sensitive data includes

- SEN records such as IEPs and Annual Review records.
- Mark sheets and assessments.
- Reports and Open Evening comments.
- Personal data stored on the School Information Management System, Capita SIMS.
- Photographic or video material.
- Name, address and contact information

Non-Sensitive data thus includes

- General teaching Plans.
- Curriculum materials
- General correspondence of a non-personal nature.

Security of Sensitive Data

- The school upholds a secure site license
- All users are responsible for only accessing, altering and deleting their own personal files. They must not access, alter or delete files of another user without permission.
- Special Categories of personal data
    - Must be encrypted on laptops.
    - Should not be emailed between personal email accounts, unless using secure email methods and complying with the Data Protection Policy.
    - Should not be put on any other removable media unless it is encrypted. Memory sticks are not permitted to be used on the school network.

Email and messaging guidance

- Staff but not pupils may use web based email accounts from school; bearing in mind that web based email cannot be monitored for unsuitable content.
- Learners should immediately tell a teacher if they receive an offensive e-mail or message or find an inappropriate web page.
- Learners should not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone via an e-mail or message.
- Emails sent by pupils to an external organisation should be authorised by a member of staff before sending.
- The forwarding of chain letters, jokes, etc. is prohibited.
- Learners may only use approved e-mail or message accounts on the school system.

Confidential Information on Laptops

In addition to the information above the following security measures should be taken with staff laptops:

- Laptops must be out of view when stored overnight in school. Pupil laptop tops must be stored in locked designated trolleys.
- Windows Operating System should be locked when a teacher user leaves their computer (Windows key + L)

- Laptops should never be left in a parked car, even in the boot for substantial periods of time.
- At home, other members of teachers' families should not use a teacher's laptop perhaps allowing access to confidential information.
- School insurance cover does not include off site accidental damage.
- Staff must sign a Laptop Agreement to take a laptop off the school site. The agreement refers to the conditions above.

Confidential Information on Paper

Staff should take care not to leave printed documents with sensitive information open to view e.g. leaving such documents on open desks or by printers. Special Categories of Personal Data should be held in lockable storage when office staff are not present.

Backing up of data

- Data is backed up using an online storage system whereby school information is securely stored in accordance with UK Data Protection Laws.
- School has introduced a system whereby staff data is synchronised to the school servers when users rejoin the network. The backup of personal data is not the responsibility of the school.
- The school works with their ICT support partner to establish business continuity systems should the network fail which would take effect to enable key school systems to quickly be reinstated. The current IT support contract supplier is Soft Egg.

The School Learning Platform

- The school Learning Platform includes the school address, school email, telephone and fax number including the school's emergency email address.
- Staff or Learners' home information is not published.
- Photographs of children are only shown with parental consent. See **Appendix Bvi**
- Personal information is not published alongside photographs of children.

The copyright of all material posted must be held by the school or be clearly attributed to the owner where permission to reproduce has been obtained or given e.g. via Creative Commons licencing

The Internet

- The school takes all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school cannot accept liability for the material accessed, or any consequences of Internet access.
- All pupils using the internet are made aware of the school's e-Safety Guidelines. These are posted near to the computer systems.
- Instruction in responsible and safe use of Internet access is provided on a regular basis (at least once each term).
- Filtering will be carried out by RM (Research Machines) as part of the managed service.
- School Staff audit ICT provision regularly to establish if the e-Safety policy is adequate and that its implementation is effective.

Course of action if inappropriate content is found

- Inappropriate web content is defined as content that is: pornographic, violent, sexist, racist or horrific. In the case of a pupil/adult accidentally viewing this content, they should:-
    - Turn off the monitor or minimise the window.
    - Report the incident to the teacher or responsible adult.
- The teacher will
    - Ensure the well-being of the pupil.

    - Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the pupils).
    - Report the details of the incident to the e-safety officer.
- The e-Safety officer will
    - Log the incident and take any appropriate action.
    - Where necessary report the incident to our Internet Service Provider (RM) so that action can be taken.

The use of new technologies

- Learners are not allowed access to public or unregulated chat rooms.
- Emerging technologies will be examined for educational benefit and a risk assessment is carried out before use in school is allowed.
- Personal mobile phones may not be used during lessons or formal school time.

Staff use of Social Networking

Please refer to the School Social Networking policy – **Appendix D**.

Use of mobile devices

- Pupils are not allowed to bring mobile phones to school unless prior arrangements are made with the school. These will then be stored in the office in accordance with our School Social Networking Policy – refer to Appendix B.
- Pupils are not allowed to bring in games devices which allow ad hoc networks to be established.
- Teacher/parent contact is by the main school telephone and not via a mobile device except where prior permission is given by the Head Teacher.
- Visitors/volunteers to school and staff are not permitted to use their mobile phones within curriculum areas. Clear signage shows where phones must not be used. Designated areas at Reception and in staff areas permit the use of phones. Parents and staff are reminded if seen using a mobile phone in prohibited areas.
- Staff and pupils may send educational messages during lesson times if these are part of the curriculum.
- Staff are not permitted to use their mobile phone in the classroom.
- Staff, volunteers and visitor mobile devices should be stored securely and out of sight during lesson time and be placed on silent or switched off.
- The school cannot take responsibility for the content of any device that is brought onto the school site which may be inappropriate or illegal.
- If staff are expecting an urgent call, they are permitted to leave their phone with the office who can call them should the call be received.

Photography of pupils

- Parents, staff and pupils are welcome to take photographs of pupils at school under the following conditions
    - Photographs must not be distributed beyond either the school or the immediate family and friends of the child's family.
    - Photographs must not be posted on an open internet site
        - On a social networking page with the permissions set to public.
        - On the school learning platform on an open page.

- No photographs of pupils can ever be taken
    - In the toilets or wash areas.
    - Whilst pupils are getting changed.
    - Whilst a child is receiving medical attention.

- Photographs are stored securely within the server on the school site and backed up via the authorised on line system.
- To ensure continued security, photographs of children are not allowed to be removed from the school site unless stored on an encrypted school laptop. Memory sticks are not permitted.
- All devices capable of taking photographs, whether belonging to the school or personal, may be subject to scrutiny by members of the SLT if required.
- Photographs of children must only be taken on approved school technology.

Acceptable Use Agreement

- All users of the school computers sign the appropriate acceptable use policy. This includes staff, pupils and parents who sign on behalf of their children. Parents will be asked to sign on behalf of their children on a regular basis.
- Please refer to Appendices regarding Acceptable Use at end of policy.

Complaints Regarding Internet Use

- The school has a procedure in place for dealing with all complaints.
- Complaints of a child protection nature are dealt with in accordance with school Child Protection policy and procedures.
- Pupils and parents can request access to the Complaints procedure.

Sanctions

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. This would constitute a disciplinary matter as far as staff are concerned.
- Please refer to Staff and Pupil AUP in the attached Appendices.

Parental Support

- Parents are made aware of the school's policies regarding e-Safety and Internet use.
- Internet issues are handled sensitively to inform parents without undue alarm.
- The School is committed to a partnership approach with parents. This may include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet can be made available to parents.

Woodley C of E Primary School
e-safety rules for Key Stage 1

Think then Click

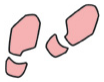
These rules help us to stay safe on the Internet

We only use the internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.



We can send and open messages together.

We can write polite and friendly messages to people that we know.

We tell a teacher/adult if anything on a computer worries us.

Woodley C of E Primary School e-safety rules for Key Stage 2

Think then Click

- We only use the internet with adult permission.
- We only use websites that an adult has approved.
- We immediately close any webpage we are uncomfortable with.
- We tell an adult if we see anything we are not sure of.
- We only e-mail people an adult has approved.
- We communicate politely and with respect when using email, forums and writing on the learning platform pages.
- We never share or display personal information (e.g. address, phone numbers)
- We never share passwords with anyone except appropriate staff.
- We only login as ourselves.
- We never arrange to meet anyone we don't know.
- We do not open messages sent by anyone we don't know.
- We do not use Internet chat rooms.
- We only upload appropriate copyright free images that have been approved, to pages on the Learning Platform and within the school environment.
- WE WILL TELL AN ADULT IF WE KNOW OF ANYONE NOT FOLLOWING THESE RULES.

Woodley C of E Primary School

e-Safety Rules

These e-Safety Rules help to protect children and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- Irresponsible use by children may result in the loss of their network, learning platform or Internet access rights.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected. This means that if children want to use Images, Media e.g. music or video, in their work, it must be only from approved websites defined by the learning platform.
- Messages will be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the Head Teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place.

Woodley C of E Primary School

e-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil:	**Class:**

Child's Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:	**Date:**

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that children cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	**Date:**

Please print name:

Please complete, sign and return to the School office