Woburn Lower School

E-safeguarding Policy

Aims of the Policy

- To set out the key principles expected of all members of the school community at Woburn Lower School with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff of Woburn Lower 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.

Scope of the Policy

- This policy applies to the whole school community including Woburn Lower School staff, school board of governors, all staff employed directly or indirectly by the school and all pupils.
- Woburn Lower School's Headteacher and school board of governors will ensure that any relevant or new legislation that may impact upon the provision for eSafeguarding within school will be reflected within this policy.

Review and ownership

- The school has appointed an eSafeguarding coordinator who will be responsible for document ownership, review and updates. This is the Headteacher.
- The eSafeguarding policy is current and appropriate for its intended audience and purpose.
- The school eSafeguarding policy has been agreed by the staff and approved by governors.
- The eSafeguarding policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The School has appointed a member of the governing body to take lead responsibility for eSafeguarding.
- All amendments to the school eSafeguarding policy will be discussed in detail with all members of teaching staff.

Communication Policy

- Woburn Lower School headteacher will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school eSafeguarding policy and the use of any new technology within school.
- The eSafeguarding policy will be provided to and discussed with all members of staff formally.
- All amendments will be published and awareness sessions will be held for all members of the school community.
- An eSafeguarding or eSafety module will be included in the ICT curricula covering and detailing amendments to the eSafeguarding policy.

- An eSafeguarding or eSafety training programme will be established across the school to include a regular review of the eSafeguarding policy.
- The key messages contained within the eSafeguarding policy will be reflected and consistent within all acceptable use policies in place within school.
- eSafeguarding posters will be prominently displayed around the school

Roles and responsibilities

We believe that eSafeguarding 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 learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Headteacher

- To promote an awareness and commitment to eSafeguarding throughout the school
- To be the first point of contact in school on all eSafeguarding matters
- To take day-to-day responsibility for eSafeguarding within school and to have a leading role in establishing and reviewing the school eSafeguarding policies and procedures
- To have regular contact with other eSafeguarding committees, e.g. the local authority, Local Safeguarding Children Board and attend appropriate courses
- To communicate regularly with school technical staff – Partnership Education
- To communicate regularly with the designated eSafeguarding governor
- To create and maintain eSafeguarding policies and procedures
- To develop an understanding of current eSafeguarding issues, guidance and appropriate legislation
- To ensure that all members of staff receive an appropriate level of training in eSafeguarding issues
- To ensure that eSafeguarding education is embedded across the curriculum
- To ensure that eSafeguarding is promoted to parents and carers
- To ensure that all staff are aware of the procedures that need to be followed in the event of an eSafeguarding incident
- To ensure that an eSafeguarding incident log is kept up to date

Responsibilities of teachers and support staff

- To read, understand and help promote the school's eSafeguarding policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any suspected misuse or problem to the eSafeguarding coordinator
- To develop and maintain an awareness of current eSafeguarding issues and guidance
- To model safe and responsible behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, **NEVER** through personal mechanisms, e.g. email, text, mobile phones etc.
- To embed eSafeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology
- If a member of staff becomes aware of an incident of sexting appropriate measures will be taken by the school

Responsibilities of technical staff

- To read, understand, contribute to and help promote the school's eSafeguarding policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy

- To report any eSafeguarding related issues that come to your attention to the headteacher
- To develop and maintain an awareness of current eSafeguarding issues, legislation and guidance relevant to their work
- To support the school in providing a safe technical infrastructure to support learning and teaching
- To liaise with the local authority and other appropriate people and organisations on technical issues
- If a member of staff becomes aware of an incident of sexting appropriate measures will be taken by the school

Responsibilities of pupils

- To 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
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school
- To discuss eSafeguarding issues with family and friends in an open and honest way

Responsibilities of parents and carers

- To help and support the school in promoting eSafeguarding
- To read, understand and promote the school pupil eSafeguarding policy
- To 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
- To discuss eSafeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children's use of technology
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images outside of school
- To sign a home-school agreement containing the following statements:
  - *We will support the school approach to online safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community*
  - *We will support the school's stance on the use of ICT and ICT equipment*
  - *Images taken of pupils at school events will be for personal use only and not uploaded or shared via the internet*
  - *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 social networking sites*
  - *Parents and carers are asked to read through and sign acceptable use agreements on behalf of their children on admission to school*
  - *Parents and carers are required to give written consent for the use of any images of their children in a variety of different circumstances*

Responsibilities of the governing body

- To read, understand, contribute to and help promote the school's eSafeguarding policies and guidance
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils
- To develop an overview of how the school ICT infrastructure provides safe access to the internet

- To 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
- To ensure appropriate funding and resources are available for the school to implement its eSafeguarding strategy

Managing digital content

- Written permission from parents or carers will be obtained for the following locations before photographs of pupils are published. This will be done annually or as part of the home-school agreement on entry to the school.
  On the school website
  On the school's learning platform
  In the school prospectus and other printed promotional material, e.g. newspapers
  In display material that may be used around the school
  In display material that may be used off site
- Parents and carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.
- Parents may take photographs at school events: however 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 social networking sites.

Storage of images

- Any images, videos or sound clips of pupils must be be stored on the school network and never transferred to personally owned equipment.
- Staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.

Learning and teaching

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 eSafeguarding-related lessons in every year group/specific year groups as part of the ICT curriculum.
- We will discuss, remind or raise relevant eSafeguarding 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.
- 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.

Staff training

- As part of the induction process all new staff will receive information and guidance on the eSafeguarding 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 eSafeguarding 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 eSafeguarding 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.
- 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 end-user 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, pupils will access the internet using a class id and password, which the teacher supervises. 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 an individual user account with an appropriate password which will be kept secure, in line with the pupil Acceptable Use Policy. They will ensure they log out after each session.
- Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. They will abide by the school AUP at all times.

Passwords

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- Key Stage 1/2 pupils will have a generic 'pupil' logon to all school ICT equipment.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All information systems require end users to change their password at first log on.
- Users should be prompted to change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.
- Users should change their passwords whenever there is any indication of possible system or password compromise
- All staff and pupils have a responsibility for the security of their username and password. Users 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.
- All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords e.g.
    - Do not write down system passwords.

- Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
- Always use your own personal passwords to access computer based services, never share these with other users.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Never save system-based usernames and passwords within an internet browser.

- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the school's personal data policy.
- Passwords must contain a minimum of eight characters and be difficult to guess.
- Users should create different passwords for different accounts and applications.

Users should use numbers, letters and special characters in their passwords (! @ # $ % * ( ) - + = , < > : : " '): the more randomly they are placed, the more secure they are.

Emerging 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 safeguarding point of view. We will regularly amend the eSafeguarding policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause a eSafeguarding risk.

- 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 deployed within school will be documented within the eSafeguarding 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 eSafeguarding and Acceptable Use policies..
- The school will audit ICT equipment usage to establish if the eSafeguarding policy is adequate and that the implementation of the eSafeguarding 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.

Filtering and monitoring online activity

The school uses a filtered internet service. The filtering system is provided by E2BN.
The school's internet provision will include filtering appropriate to the age and maturity of pupils.

The governing board ensures the school's ICT network has appropriate filters and monitoring systems in place. The governing board ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The Headteacher and ICT technicians (Partnership Education) undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

Requests regarding making changes to the filtering system are directed to the Headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL conduct a risk assessment. Any changes made to the system are recorded by ICT technicians. Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices are appropriately monitored. All users of the network and school-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the Child Protection and Safeguarding Policy.

Email

- Pupils may only use school-provided email accounts for school purposes.
- Staff are not permitted to access personal email accounts during school hours.
- Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents.
- Whole class or group email addresses will be used in school for communication outside of the school.
- Access, in school, to external personal email accounts may be blocked.
- Email from staff are sent via the school's email and never via personal email.
- It is the responsibility of each account holder to keep the password secure.
- School email accounts should be the only account that is used for school-related business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

Mobile phone usage in schools

- 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, except for emergency usage.
- 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.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within school or on trips unless under emergency conditions.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used. In an emergency where the staff member doesn't have access to a school owned device, they should use their own devices and hide (by inputting 141) their own mobile numbers for confidentiality purposes.

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 and GDPR 2018.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR 2018.
- 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.
- Any access to personal and sensitive information should be assessed and granted by the **Data Protection Leads, the Headteacher and Emma Lunn**. (SIRO and the applicable IAO)
- All access to the school information management system will be on a need-to-know or least privilege basis. All access should be granted through the above.
- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis. All access should be granted through the above.
- 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.
- Document backed up daily by cloud storage supplied by Partnership Education.
- 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 full disk, encrypted removable media, remote access over encrypted tunnel.
- 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.
- Woburn Lower School has a data sharing agreement with Central Bedfordshire.

Related policies:

Acceptable Use
Safeguarding
Peer-on-peer abuse (child-on-child abuse from September 2022)
Behaviour
Data Protection
Whistleblowing
Online Safety

Governor:

Date: January 2024

Headteacher:

Date: January 2024

Review: January 2025