Online Safety Policy

Approved by Education and Standards Committee July 2022

Introduction

Our children are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. **Online Safety** is about acknowledging the positive and enriching side of digital life whilst recognising its challenges and being aware of the nature of the possible risks that could be encountered and how to best manage them.

Online Safety is an integral part of safeguarding and as such this policy should be read in conjunction with our **Child Protection and Safeguarding Policy**. Links with other policies include, but are not limited to: Behaviour Policy, Curriculum Policy, Data Protection Policy, Remote Learning Policy and Whistleblowing Policy.

Aims

This policy aims to:

- Set out our commitment to safeguarding children online and protecting them from potentially harmful and inappropriate materials
- Make all stakeholders aware of their roles and responsibilities regarding online safety
- Set out the expectations for how our community members should use the internet safely
- Identify reporting channels for concerns and online safety incidents

Roles and Responsibilities

Wilbury Primary School is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, children, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

The following section outlines the online safety roles and responsibilities of individuals and groups within our community:

All Staff

All members of school staff (teaching and non-teaching) have a responsibility to protect children online. This includes every member of staff who works at the school; headteacher, teachers, supply teachers, work-experience staff, office staff, nurses, caretakers, cleaners, etc. All teachers and staff must always act in accordance with their own professional boundaries, upholding professional behaviour and conduct at all times.

All school staff need to:

- Be aware of and adhere to all policies in school which support online safety and safeguarding including signing the staff acceptable use policy (Appendix 1)
- Contribute to policy development and review.
- Support in the ownership and responsibility for the security of systems and the data accessed.
- Model good practice when using technology.
- Know the process for making referrals and reporting concerns.
- Know how to recognise, respond and report signs of online abuse and harm.
- Receive appropriate child protection training.
- Always act in the best interests of the child.
- Be responsible for their own continuing professional development in online safety.

Children

With respect to online safety, children should:

- Read, understand, sign and adhere to the school's Acceptable Use Policy (Appendix 2 & 3)
- Engage in age-appropriate online safety education opportunities
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff
- understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's AUP covers actions out of school, including on social media

Parents / Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' meetings, newsletters, the school website and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and:

- Read and promote the AUP and encourage their children to follow it
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers
- Be responsible when taking photos/using technology at school events.
- Identify changes in children's behaviour that could indicate they are at risk of online harm or abuse
- Know how to report online issues and consult with the school if they have any concerns about their children's and others' use of technology

Trustees

The board will:

- Uphold online safety as a safeguarding issue which is embedded across the whole trust
- Evaluate and approve this policy at each review, ensuring it complies with the law, and hold the headteacher to account for its implementation
- Appoint a senior board level (or equivalent) lead or, link governor to monitor the effectiveness of this policy in conjunction with the full governing board

Local Governing Body

Governors on local governing bodies will review the school specific elements of the policy after the trust level policy has been reviewed and approved. They will:

- appoint a member of the local governing body to act as the governor responsible for safeguarding including online safety
- Uphold online safety as a safeguarding issue which is embedded across the whole school culture.
- Ensure that children are provided with a safe environment in which to learn and develop.
- Ensure the school has effective policies and training in place.
- Audit and evaluate online safety practice including carrying out risk assessments on the effectiveness of filtering systems.
- Ensure there are robust reporting channels.

Headteacher

The headteacher is responsible for the implementation of this policy, including

- Communicating this policy to parents/carers when their child joins the school and via the school website
- Overseeing the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Liaising with the DSL on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Ensuring that policies and procedures are followed by all staff
- Ensuring that the school has appropriate filters and monitoring systems in place
- Fostering a culture where online safety is fully integrated into whole-school safeguarding

Designated Safeguarding Lead

With respect to online safety, it is the responsibility of the DSL to:

- Promote online safety and the adoption of a whole school approach
- Liaise with the Computing and RSE leads to ensure children are being appropriately taught about and know how to use the internet safely and responsibly
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident
- Ensure staff and parents are aware of measures to keep children safe online through relevant training provision
- Facilitate effective record keeping and the reporting and monitoring of all online safety concerns.
- Meet regularly with Computing Lead and IT Technician to discuss current issues and review filtering and monitoring reports
- Maintain own training and learning needs, ensuring they are up to date with all matters relating to online safety.

Computing Lead

With respect to online safety, it is the responsibility of the Computing Co-ordinator to:

- Ensure children and young people are being appropriately taught about and know how to use the internet safely and responsibly
- Work closely with the RSE lead to avoid overlap but ensure a complementary whole-school approach and ensure all staff understand the issues, approaches and messaging within Computing
- keep up to date with the latest risks to children whilst using technology; be familiar with the latest research and available resources for school and home use
- Engage with parents and the school community on online safety matters at school and/or at home
- Ensure any technical online safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the IT Technician and ICT Technical Support

- Meet regularly with the DSL, IT technician and ICT Technical support to review issues arising, audit filtering and monitoring reports and plan for appropriate responses including training and education of children, staff and parents
- Work with the Headteacher to ensure the school website contains relevant information for staff, children and parents regarding online safety

IT Support / Technician

Those with technical responsibilities are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That users only access the networks and devices through a properly enforced password protection policy
- Ensure any technical online safety measures in school are fit for purpose and monitor its implementation, sharing reports with the Computing Co-ordinator and the DSL as appropriate
- That they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant

Policy Statements

Acceptable Use

Use of digital technology in school is a privilege, not a right. The school seeks to ensure that digital technologies are used safely by all users and for their intended educational purposes. All users are required to read and sign an Acceptable Use Policy which provides a framework for such use (appendix).

Handling Online Safety Concerns and Incidents

Online safety is a part of safeguarding, and as such, all concerns should be dealt with in the same way as detailed in the **Child Protection and Safeguarding Policy.** In short, all concerns must be logged and reported to the DSL.

All Online Safety incidents should be reported to a DSL and recorded appropriately on the CPOMS (or equivalent software) electronic recording system. All heads of department are part of the designated team and as such should be the first point of contact. Incidents will be dealt with in accordance with the school **behaviour policy.**

The DSL and the computing coordinator will meet regularly to identify any further actions required in response to incidents.

Any concerns regarding the conduct of staff or volunteers should be reported to a line manager or headteacher as detailed in the Whistleblowing Policy.

Education and Training

Children

Online Safety education is an essential part of the school's online safety provision. Through a carefully planned online safety curriculum children will learn the key skills required to safely navigate the challenges and risks presented online. As identified in [Teaching Online Safety in School 2019](#) it is important to teach children the underpinning knowledge and behaviours that will help them to navigate the online world safely and confidently. These include:

- **How to evaluate what they see online** – enable children to consider carefully the information that is available to them and consider its validity
- **How to identify online risks** – support children to identify possible online risks and how they might deal with them
- **Online behaviour –** support children in understanding what acceptable and unacceptable online behaviour looks like and that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others
- **How to recognise techniques used for persuasion** – help children to identify methods through which online content and users seek to manipulate their online behaviour

- **How and when to seek support –** ensure children know how to report their concerns and where to get support if they are concerned or worried

This online safety curriculum will be regularly reviewed and will be guided and put together using the most recent and up to date frameworks and resources. For example, The Education for a Connected World Framework, Project Evolve and CEOP's Thinkuknow resources.

Alongside this discrete online safety education, it is the role of all staff to identify opportunities to thread online safety through all school activities and make the most of unexpected learning opportunities as they arise. Whenever overseeing the use of technology in school or setting as homework tasks, all staff should encourage sensible use, monitor what children are doing and consider potential dangers and the age appropriateness of websites.

All staff should supervise and guide children when engaged in learning activities involving online technology supporting them with search skills, critical thinking (e.g. fake news), age-appropriate materials and legal issues such as copyright.

Parents / guardians

Parents play the most important role in the development of their children. As such, the school will support parents to have the skills and knowledge they need to ensure the safety of children outside the school environment. Using:

- Information leaflets
- Newsletters
- the school's website
- parents' meetings
- Signposting to relevant web sites and publications

The school will work alongside parents to ensure they know how to help children stay safe, how to report concerns regarding online safety and are made aware of new and emerging risks.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. Pupils sign an age-appropriate Acceptable Use Policy which sets out how they should use the available technology in school. Parents can view these policies through the school website and should encourage children to follow it.

Staff

It is important that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Online safety training will be regularly made available to all staff, if individuals feel they require further training this should be addressed through their performance management or by approaching the DSL or Computing Coordinator directly.

Device Usage

Wilbury Primary School will endeavour to provide up to date technology for the use of staff and children as appropriate to support teaching and learning. These devices are to be used in accordance with the Acceptable Use Policy which includes, but is not limited to:

- Using devices for educational purposes and acknowledging that all usage may be monitored
- Only using your own username and password to access devices
- Only using school owned devices for recording videos/pictures – personal devices should not be used
- Ensuring devices are locked and password protected when left unattended

Mobile Phones

- Children should not bring mobile phones into school. Children in KS2 Upper who walk home alone are allowed to bring a mobile phone with them for the purposes of communication. However, these are switched off at the start of the school day, given to a member of staff and returned at the end of the day.
- Staff bringing in mobile devices should ensure they are not left unattended where they may be accessed by children or other persons

Staff Using School Devices Out of School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates

If staff have any concerns over the security of their device, they must seek advice from the computing co-ordinator or IT support.

Children Using School Devices Out of School

All children borrowing a school device are required to sign an Acceptable Use Policy (appendix). These devices should be used to support learning and are not subject to the same filtering and monitoring available in school. Parents should therefore be made aware of this and take appropriate steps to ensure the safe use of the device (advice and support on how to do this is available through the school's website).

Communication

Email

All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Personal email addresses should not be used for work purposes.

Staff should consider carefully the information they share through email and be alert to spam and phishing scams which request personal information. Any such communications should be reported to the computing coordinator and data protection officer.

Children do not have access to a school email address.

Social Media

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and children will use it. However, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups

Children

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school regularly deals with issues arising on social media. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our children to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse.

Children are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Children are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

Staff

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

---

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Use of Digital and Video Images

The use of digital media, such as photographs and videos, is permitted in accordance with the following:

- parental / carer permission is given for use of digital photographs or video involving their child
- Children will not be identified in online photographic materials or have their full names included in the credits of any published school produced video materials
- Staff can take digital/video images to support educational aims but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used
- Children are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.
- Children are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Children are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

Notice and take down policy

Should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Technical – infrastructure/equipment, filtering and monitoring

To make the school infrastructure/network as safe and secure as reasonably possible:

- The school has educational filtered secure broadband connectivity through the London Grid for Learning (LGFL) and so connects to the 'private' National Education Network. This includes the LGFL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. The Computing Coordinator and IT Support are responsible for ensuring that the filtering is appropriate and reports are regularly checked so that any issues are brought to the attention of the DSL and Headteacher.
- The school's email is provided through Microsoft Office 365 which provides robust email protection against spam, viruses, and malware with Exchange Online Protection.
- All capable devices will have anti-virus software installed. We currently use Sophos antivirus software (from LGFL) which is automatically updated. IT Support will be responsible for

ensuring it is updating and protecting the network and will report to the Computing Co-ordinator and / or the Headteacher if there are any concerns.

- Any actual/potential technical incident/security breach should be reported to the computing coordinator / headteacher as soon as possible.
- All users will have clearly defined access rights to school technical systems and devices.
- All devices should require a username and password to be used:
  - o Staff have a unique username and password which they use to access devices and have a responsibility for the security of this information. Users should not allow other users to access the systems using their log on details.
  - o Children in Key Stage one have a unique username and a generic password which they use to access devices. In Key Stage 2 pupils have a unique username and password. Children are prompted to change their password at the beginning of each school year.

Data Protection

With regards to Data Protection, all member of Wilbury Primary School will adhere to the Trust's Data Protection Policy. Which includes, but is not limited to, ensuring that:

- at all times care is taken to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- They will immediately contact the Data Protection Officer if there has been, or they are concerned there may have been, a data breach.
- Papers containing confidential personal data, including login details and passwords, must not be left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Passwords must be used to access school devices. These must also be in use on personal devices which have access to school information e.g. email or cloud storage. These devices should also lock when unattended.
- Staff are encouraged not to use removable devices to store/transfer personal information. However, if they are used then they must be encrypted and password protected.

Acceptable Use Policy – Staff and Volunteers

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people

I understand that the school digital technology systems are intended for educational use only

I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials. Inadvertent access must be treated as an online safety incident and be reported to the Computing Coordinator

I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.

I will only communicate with children and parents/carers using official school systems. Any such communication will be professional in tone and manner

I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

I will ensure that if I take and/or publish images of others I will do so with their permission and I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

I will not engage in any on-line activity that may compromise my professional responsibilities.

I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

I will not store school-related data on my personal devices, storage or cloud platforms. USB memory sticks, if used, will be encrypted.

I will ensure my personal devices are password protected and lock when unattended to prevent access to school online platforms e.g. email or cloud storage.

I will immediately report any damage or faults involving equipment or software however this may have happened.

I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Line Manage / Headteacher (if by an adult)

I understand that breach of this AUP and/or of the school's full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:

Acceptable Use Policy – Children KS2

Wilbury Primary School will try to ensure that children have good access to ICT to enhance their learning and will, in return, expect the children to agree to the following:

✓ I am responsible for my own behaviour including the language I use and the materials I choose to access.

✓ I understand that my use of the internet is monitored

✓ I will use hardware in school considerately and report any problems to an adult

✓ I will only log into computers using my username and password

✓ I will always keep my personal information safe

✓ I will not intentionally access unsuitable material and if I do by accident I will inform an adult

✓ I will be polite and responsible when I communicate with others online and treat other users with respect

✓ I will remember that stranger danger also applies online

✓ I will not download files from the internet without permission

✓ I understand that failure to behave appropriately will be dealt with according to the school behaviour policy.

Name:

Acceptable Use Policy – Children KS1

I will take care of the computers and other equipment

I will only use activities that a teacher or suitable adult has told or allowed me to use

I will be careful what I click on when using the internet

I will ask for help if I'm stuck or not sure

I will tell a trusted adult if I'm upset, worried, scared or confused

I will always keep my personal information safe

I look out for my FRIENDS and tell someone if they need help

I will be kind and polite to others online

I know that if I break the rules, I might not be allowed to use a computer

Name:

Appendix 4

This policy was created using information from the policy templates:

SWGFL Online Safety Policy Template:

Free Online Safety Policy Templates for Schools | SWGfL

LGFL Online Safety Policy Template:

Online Safety Resource Centre - London Grid for Learning (lgfl.net)

National Online Safety:

National Online Safety | Keeping Children Safe Online in Education

The Key Support Services

Online safety policy: model and examples | The Key Leaders (thekeysupport.com)

Computing Device Loan Agreement – Children

Wilbury Primary School is lending you a device to use for educational purposes. In return you are agreeing that:

✓ I will use the device for educational purposes: like completing my home learning

✓ I am responsible for my own behaviour including the language I use and the materials I choose to access.

✓ I will only log into computers using my username and password

✓ I will always keep my personal information safe

✓ I will not intentionally access unsuitable material and if I do by accident, I will inform an adult

✓ I will be polite and responsible when I communicate with others online and treat other users with respect

✓ I will remember that stranger danger also applies online

✓ I will not download files from the internet without permission

✓ I will return the computer in the same condition as I received it

Name: