WRAY COMMON PRIMARY SCHOOL

Online Safety Policy

Governors' Committee Responsible: Teaching and Learning Committee
Governor Lead: Chris Brown
Nominated Lead Member of Staff: Ashleigh Fanner
Status & Review Cycle: Statutory & Annual
Next Review Date: Spring 2027

Aims:

- To ensure all staff adopt safe practices in the use of the internet and in the teaching of internet use to children.
- To educate children to be responsible and informed internet users.
- To inform and support parents in keeping their children safe on the internet at home, on PCs or other internet-enabled devices, e.g. consoles, smartphones and tablets.

Online safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for safeguarding, anti-bullying, data handling and using photographic images of children seeking your consent. It also relates to the Staff and Governor Acceptable Use Agreement.

Using this policy

- Online safety will be one of the focuses of the safeguarding team. There will be an appointed online safety co-ordinator which will usually be the computing lead, working closely with the DSL.
- Our online safety policy has been written by the school, building on best practice and government guidance. It has been agreed by the senior leadership team and approved by governors.
- The online safety policy was revised by: Ashleigh Fanner 4th March 2026
- The online safety policy covers the use of all technology which can access the school network and the internet, or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand-held games consoles used on the school site.
- The online safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks for staff via school PCs and laptops will be controlled by personal passwords which are changed termly.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform online safety policy.
- The DSL is responsible for monitoring suspicious or inappropriate use
- All adults are expected to report any concerns about what children are searching to the DSL.
- Any inappropriate or suspicious searches are flagged to DSL and IT technician and are logged and followed up on.
- The security of school IT systems will be reviewed regularly.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored using Arista.
- Pupils access laptops via individual log-ins and the school network on tablets via tablet specific log-ins.

Online Safety curriculum

The school will provide an age-appropriate online safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. Online safety is taught from Reception - Year 6 during the Spring Term as part of PSHE learning but also throughout the year as a 'drip fed' approach during computing lessons and through Online Safety Assemblies run by the Computing lead. The SMART with a heart rules are taught as well as learning under the following headings:

Online safety
Privacy and security
Online Relationships
Online health, wellbeing and lifestyle
Online self-image
Online reputation
Managing online information
Online copyright

As part of the curriculum, pupils are advised not to give out personal details or information which may identify them or their location and to ensure privacy settings are turned on for social media websites and apps.

Pupils will be taught how to recognise unpleasant internet content and the procedures for reporting to adults.

E-mail

- Staff may only use approved e-mail accounts on the school IT systems.
- Staff have two-factor authentication set up to access emails which is reset at least every 40 days for each device a member of staff uses, to access their emails.
- Staff email accounts must not be used for personal reasons.
- All school communication must only take place via the school email system, where communication is sensitive Egress switch is used for emails.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known. If members of staff believe they have been sent a phishing email or an email from an unknown email address, members of staff must report to the School Business Manager and forward onto the School IT Technician.

Published content e.g. school website, newsletter, social media

The contact details will be the school address, email and telephone number. Pupils' personal information will not be published and staff names only will be published.

The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Digital work created by pupils may be put on the school website, Instagram page or private YouTube channel with first names only and no other personal information including images of children will appear.

Consent via an online form will be obtained from parents or carers before photographs or full names of pupils are published on the school website or any school run social media as set out in Surrey Safeguarding Children Partnership Guidance on using images of children. The consent is registered on Arbor as to whether the child has permission for individual/ sibling photos to be taken and/or whether photos of the child can be used in the newsletter or on any school social media sites.

Use of social media

- The school will block access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their position as a member of the school community.

Response to children sending and/or receiving nudes and semi-nudes

- Our safeguarding policy states the school's response to how it will deal with any identification that an incident of sexting and/or youth produced sexual imagery may have occurred.
- Additionally, the safeguarding policy alongside the behaviour policy, as a reference to apply a sanction where necessary, states the set procedures and sequences that must be initiated should staff suspect.

Use of personal devices

- Personal devices within school should not have access to the school Wi-Fi network.
- Mobile phones must be password protected by a code-lock.
- Staff must not take images of pupils or store pupil personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.
- Children in Years 5 and 6 are allowed to bring mobile phones to school. This requires a written request from their parents. These requests are considered by the SLT who may or may not grant permission. Mobile phones must be handed into the class teacher and then stored at the office at the beginning of the day and collected at the end. Permission can be withdrawn for improper use such as 'Sexting.'

Protecting personal data

The school has a separate Data Handling Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site, remote access to school systems. Off-site access is available for all staff via Microsoft Teams system which is password protected. USB sticks are not to be used by staff/ external staff in school.

Remote Learning

- During periods of partial or full school closures, when children have access to live and recorded lessons, children and parents will be reminded of the school's Code of Conduct for Remote Learning.
- Parents will be asked to give their consent digitally, to the Staff Code of Conduct for Remote Learning, for their child's participation in remote learning.
- Safety procedures as set out in "Contingency Plan for Remote Learning" will be followed.

Policy Decisions

Authorising access

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians and governors) must read and sign the 'Staff Code of Conduct'; Acceptable Use Policy and ICT Code of Conduct; and Data Protection and Cyber Security Guidance before accessing the school IT systems.
- The school will maintain a current record of all external staff who are granted guest access to the school network.
- At Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific and approved on-line materials.
- At Key Stage 2, access to the internet will be with teacher permission with increasing levels of autonomy.
- Children and parents are asked to sign a Computing Code of Conduct in their home school learning journals at the beginning of each school year.

People who are not employed by the school including visiting supply teachers must read and sign the Acceptable Use Policy and ICT Code of Conduct before being given access to the internet via school equipment or Wi-Fi.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school

nor Surrey County Council can accept liability for the material accessed, or any consequences of internet access.

Handling online safety complaints and issues arising from it

- Online Safety incidents recorded by designated safeguarding lead DSL.
- Complaints of internet misuse will be dealt with according to the school behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the school's behaviour policy.

Raising profile

- Parent workshops
- Promotion of online safety literature and relevant resources through newsletter and website
- Reference to Home Learning Journal
- Staff provided with point of contact, online safety curriculum and signposted to resources

Communication of the Policy

Website

- Website will provide information and suitable links for our stakeholders to reference.
- Policy will be available via the website and hardcopies available on request from the school office.

To pupils

- Pupils need to agree to comply with the pupil Computing Code of Conduct in order to gain access to the school IT systems and to the internet.
- Pupils will be reminded about the contents of the Code of Conduct as part of their online safety education and whenever using a school device (i.e. tablets, laptops).

To staff

- All staff will be shown where to access the online safety policy and its importance explained.
- All staff must sign and agree to comply with: the Staff Code of Conduct; Acceptable Use Policy and ICT Code of Conduct; and Data Protection and Cyber Security Guidance in order to gain access to the school IT systems and to the internet.
- All staff will receive online safety training annually, and PREVENT (Protecting children from extremism and radicalisation) training.

To parents

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Home Learning Journals will have a section for parents and children to sign.
- Parents' and carers' attention will be drawn to the school online safety Policy in newsletters, the school brochure and on the school website.
- Parents will be offered online safety training.

This policy also links to our policies on:

Behaviour,
Staff Handbook
Whistleblowing,
Anti-bullying,
Health & Safety
Allegations against staff,
Parental concerns,
Teaching and Learning
PSHE
Sex and Relationships Education
Safeguarding and Child Protection *Policy*