West Byfleet Infant School
We Belong, Inspire, Succeed

E-SAFETY POLICY

Context of Policy to our School vision and Values

Member of staff responsible	Computing Lead
Policy agreed/last reviewed	Spring 2025
Next review date	Spring 2026
Other Related Policies	Computing Anti-bullying Live webcam protocols
Is it a Statutory Policy?	No
Does it need Governor approval?	No

E-safety Policy

This e-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 and tablet devices used on the school site.

West Byfleet Infant School aims:

- To teach children how to use internet based games, devices, websites safely and responsibly.
- To know and recognise online bullying
- To understand what to do when they are unsure of communication or images online
- To understand the impact of online use on their wellbeing
- To know who to speak to if they experience online abuse / contact

West Byfleet Infant School ensure that our children can:

- Use the internet safely and purposefully
- Report online abuse or misuse to the correct people with greater confidence
- To know what is acceptable online and when to report it
- That pupils with SEND are given equal opportunities and an increased level of safety when using computers / online devices in school

The curriculum has been updated with the June 2019 'Teaching Children e-safety in schools' and the 2020 'Education for a Connected World' recommendations. We have chosen age appropriate objectives to be included.

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 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 will be controlled by **personal** passwords. 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 e-safety policy. The security of school IT systems will be reviewed regularly. Management of filtering systems is conducted by RM internet service and senior management will agree these filtering protocols during yearly consultations with our IT support staff. All photos are saved within folders on the server which is only accessible to school staff with a school login. No photos will be published without parent's written consent on the website.

Internet Use

The school provides an age-appropriate e-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. Age appropriate learning activities are planned to teach KS1 pupils about internet safety and who to report e-safety issues to if they have concerns.

- All communication between staff and pupils or families will take place using school equipment and/or school accounts.
- Pupils will be advised not to give out personal details or information which may identify them or their location.
- The contact details will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- Staff will take overall editorial responsibility and ensure that content is accurate and appropriate.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school IT systems.
- Incoming e-mails should be treated as suspicious and attachments not opened unless the author is known.
- Pupils will not send emails to anyone outside of the school community (KS1 curriculum does not include this).
- E-gress and Secure encryption filter will be used to share sensitive and personal information eg. Financial / SEND information.

Publishing pupils' images and work

Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school website or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children.

Use of personal devices

Although we feel that our equipment is sufficient for staff to use, personal equipment may be used by staff to access the school IT systems provided their use complies with the e-safety policy and the relevant AUP. No data, information or emails must be saved or stored on personal equipment including laptops, tablets or phones. Emails must be logged out of if using a personal device. Staff must not store images of pupils or pupil personal data on personal devices.
Watches that can receive texts / updates must not be used by staff when working with the children – same usage as a phone. The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Authorising access

The school will maintain a current record of all staff and pupils who are granted access to school IT systems. At Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials. Supply teachers will have a GUEST logon when accessing school computers – this is shared with them on arrival at the Office. Daily Smoothwall restrictions are shared with the Computing lead /DSL and Headteacher – daily report. Actions are taken if breaches are found.

Social media

Staff and pupils should use ensure that their online activity, both in school and externally, considers the feelings of others, professionalism in line with the teaching standards / teaching assistant standards and is appropriate for their situation as a member of the school community. Any abuse must be reported to the Headteacher / Computing lead asap and they will comply with online regulations and protocols to report the behaviour. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of students and staff members and the reputation of the school and the County Council are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

This policy applies to the school governing body, all teaching and other staff, whether employed by the County Council or employed directly by the school.

The policy covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school.
Staff must ensure that they use the Internet sensibly, responsibly and lawfully and that use of the Internet and social media does not compromise school information or computer systems and networks. They must ensure that their use will not adversely affect the school or its business, nor be damaging to the school's reputation and credibility or otherwise violate any school policies.

- Photographs of children will NOT be published on any social media account (school's Twitter page is our only outlet). Photographs of staff linked to in-school events may be published with their consent – list has been obtained and held by school office.
- staff members must not cite or reference pupils/students/parents in tweets

- material published must be truthful, objective, legal, decent and honest; • material published must not breach copyright; • any publication must comply with all of the requirements of the General Data Protection Regulations (GDPR) 2016 and the Data Protection Act 2018, and must not breach any common law duty of confidentiality, or any right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information;
- material published must not be for party political purposes or specific campaigning which in whole or part appears to affect public support for a political party;
- material published must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns;
- the tone of any publication must be respectful and professional at all times, and material must not be couched in an abusive, hateful, or otherwise disrespectful manner;
- publication must be in line with school policies;

Any online abuse MUST be reported and recorded on CPOMS and then Head teacher and Computing lead MUST be notified immediately.

Facebook / Whatsapp

Staff should not 'friend' current or ex- pupils within the school community. If staff are 'friends' with families within the school community, they need to maintain professional conduct and avoid any communication linked to the school. Instead, this should be conducted via the usual school communication methods. If staff members are concerned about comments on ANY social media outlet, they are to contact the Computing Lead and Head teacher immediately, who will follow the usual safeguarding protocols.

Handling e-safety complaints

Complaints of internet misuse will be dealt 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 schools' behaviour policy.

To staff

- All staff will be shown where to access the e-safety policy and its importance must be explained.
- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet

To parents

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents' and carers' attention will be drawn to the School e-safety Policy in newsletters, the annual school leaflet and on the school web site.
- Children will have an annual e-safety focus week in school and where appropriate, and possible, will take part in outside agency run workshops to promote safe internet use.
- Parents will be offered e-safety training annually

Live webcam – School Closure

See separate 'Live Webcam use protocols'