

Watchfield Primary School



E-Safety Policy 2024

“At Watchfield we SOAR”



Introduction

The e-safety policy is important in our school for a number of reasons, including:

- To ensure our students have a full understanding of how to keep themselves safe using technology online including social networking (Snapchat, Instagram etc).
- To ensure that we keep our children safe, in line with KCSIE.
- To ensure there is a clear and consistent approach responding to incidents.
- To ensure that every person responsible for the children is fully aware of his/her responsibilities.
- To set boundaries of use of any school owned IT equipment, or personal IT equipment used in the school, and set the boundaries of services such as social networking (e.g. blogging, Twitter).

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents and carers

Safeguarding is a serious matter; at Watchfield Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on a regular basis. The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Watchfield Primary School website; upon review all members of staff will sign as read and understood both the e-safety policy and the IT Acceptable Use Policy for Staff. Upon starting the school, parents and children will receive a copy of the Students Acceptable Use Policy. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Policy Governance (Roles and Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy regularly and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one safeguarding governor to have overall responsibility for the governance of e-safety at the school who will:
 - Keep up to date with emerging risks and threats through technology use.
 - Receive regular updates from the Head of School with regards to training, identified risks and any incidents.

Safeguarding Governor: Di Sheldon

Head of School

Reporting to the governing body, the Head of School has overall responsibility for e-safety within our school. The Head of School who in our school is also the E-safety Officer will ensure that:

- e-safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- All e-safety incidents are dealt with promptly and appropriately.
- Monitor e-safety breaches through the filtering system and act upon these in a timely and effective manner.

E-Safety Officer

The day-to-day duty of e-safety officer is devolved to the Head of School.

The e-safety officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the governors.
- Advise the governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, Cambrian Learning Trust IT Services and other agencies as required.
- Retain responsibility for the e-safety incident log on CPOMs; ensure staff know what to report and ensure the appropriate audit trail. Ensure any technical e-safety measures in school (e.g.

Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.

- Make him/herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the responsible governor to decide on what reports may be appropriate for viewing.
- Monitor e-safety breaches through the filtering system and act upon these in a timely and effective manner.

Cambrian Learning Trust

IT Services Staff Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum: Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer / Head of School.
- Passwords are applied correctly to all users as appropriate to age.
- The Head of School and Deputy monitor any incidents through alerting them to any internet breaches through the IT filtering system.

All staff and volunteers

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Head of School.
- Any e-safety incident is reported to the e-safety officer (and an e-safety Incident report is made using CPOMs). If you are unsure, the matter is to be raised with the e-safety officer/ Head of School to make a decision.
- Inform parents of any incident/breach to the child's Acceptable Use Policy.
- The reporting flowcharts contained within this e-safety policy are fully understood.
- They agree and adhere to the terms of acceptable use and ensure that pupils follow their acceptable use agreement

All students

The boundaries of use of ICT equipment and services in this school are given in the E-Learning Code of conduct; any deviation or misuse of ICT equipment or services will be dealt with in accordance with our Positive Relationships policy.

E-safety is embedded into our curriculum both explicitly through Computing and PSHE lessons as well implicitly through all other curriculum areas where IT is in use; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through Parent Consultations, the school website, Parentpay, Online Safety letters and school newsletters, the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such, parents will sign the student E-Learning Code of Conduct before any access can be granted to school ICT equipment or services.

Parents at Watchfield will receive a monthly e-safety newsletter highlighting Apps and games that their children may use. The newsletter states clearly the age limit of games and apps and how to adjust settings to give the highest security levels for their child/ren. Where there has been a breach to the IT Acceptable Use Policy, parents will be informed as to the nature of the breach.

Visitors and members of the community

Visitors and members of the community who use the school's ICT equipment or internet will be made aware of the terms of acceptable use.

E-safety Link Governor

The e-safety governor is responsible:

- to advise on changes to the e-safety policy.
- to establish the effectiveness (or not) of e-safety training and awareness in the school.
- To establish the effectiveness of filtering and monitoring across the school.
- to recommend further initiatives for e-safety training and awareness at the school.

EDUCATING PUPILS ABOUT ONLINE SAFETY

E-safety for students is embedded into the computing curriculum – see computing policy. Whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning, using resources such as Childnet, internet matters, thinkyouknow, and Online protection - CEOP, NSPCC.

Pupils will be taught about online safety as part of the curriculum:

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- What it means to have an online identity, how this can be shaped by online content and media and the potential consequences and impact of our digital footprints
- How to use a search engine to safely search for the desired information
- The importance of a strong password, how to create one and the need to keep it a secret
- The definition of cyberbullying, giving examples and knowing what to do if they think it is happening
- How to identify a spam email and what to do if they come across one
- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

The safe use of social media and the internet will also be covered in other subjects where relevant. Where children have additional educational needs, there may be a requirement to provide further educational experiences to reinforce the learning in order to keep them safe. This will be reviewed on an individual basis where necessary.

EDUCATING PARENTS ABOUT ONLINE SAFETY

Watchfield Primary School will raise parents and carers' awareness of internet safety in letters or other communications home, and in information via our website (Safeguarding section). This policy will also be shared with parents via the school website. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of School and/or the DDSL. Concerns or queries about this policy can be raised with any member of staff or the Head of School.

Cyber Bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school's Anti-bullying policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyberbullying, its impact and ways to support pupils, as part of safeguarding training. The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

<https://www.legislation.gov.uk/ukpga/2011/21/section/2/enacted>

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or

- Disrupt teaching, and/or
 - Break any of the school rules If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team, along with advice from our Trust and IT support provider, to decide whether they should:
- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Before searching of any device takes place, advice will be sought from our Operations Manager within the Trust. Parents would be informed at all stages.

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. A record will be kept of incident and reasons for the deletion of data / files on CPOMS. School staff will ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable Use Policy and Agreements

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (See Staff IT Acceptable Use policy and E-Learning Code of Conduct – EYFS, KS1 and KS2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the acceptable use policies (see policy documents).

Pupils Using Mobile Devices in School

Pupils In Y5/Y6 may bring mobile devices into school, but are not permitted to use them at any point during the school day. Upon arrival at school, they are required to hand them into the class teacher and they will be locked away until the end of the school day. Mobile Phones should be turned on at the end of the day, outside of the school grounds. Using mobiles phones on the school grounds to take photographs or videos on the school ground is not permitted. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school Relational Behaviour policy, which may result in the confiscation of their device until the end of the school day.

Staff Using Work Devices Outside School

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in IT Acceptable User Policy - Staff. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all

reasonable steps to ensure the security of their work device when using it outside school. All work will be accessed through the 'cloud' using sharepoint linked with their outlook emails. If staff have any concerns over the security of their device, they must seek advice from the IT Staff at the Trust. Work devices must be used solely for work activities.

Responses To Misuse

Any e-safety incident is to be brought to the immediate attention of the e-safety officer / the Head of School. The e-safety officer will assist in taking the appropriate action to deal with the incident and to fill out an incident log on CPOMS. Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour, computing and the acceptable use agreement. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Watchfield Primary School will have a programme of training as necessary which is suitable to the audience.

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation (Prevent training).
- All staff members will receive refresher training at least once each academic year as part of safeguarding training and Prevent training, as well as relevant updates as required (for example through emails, noticeboard and staff meetings).
- The DSL [and deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
- Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
- Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy. As well as the programme of training we will establish further training or lessons as necessary in response to any incidents. The e-safety officer is responsible for recommending a programme of training and awareness for the school year. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Head of School for further CPD.

Technology

Watchfield Primary School uses a range of devices including PCs, laptops, Chrome books and i-pads. In order to safeguard the students and in order to prevent loss of personal data, we employ the following assistive technology:

Internet Filtering – This prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The e-safety officer and IT Services are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head of School who will pass this information onto the IT team.

Internet Monitoring – The Head of School and Deputy Head of School, receive emails daily (suicide monitoring) and weekly (general filtering of words/phrases of concern) to monitor breaches of filtering. Any breaches are acted upon immediately. Contact will be made by the Head of School/Deputy Head of School to the Trust Operations and IT team of any breaches of internet filtering.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are password protected. No data is to leave the school on a device without a password; it is all stored on the cloud and should be accessed this way. Any breach (i.e. loss/theft of device such as laptops) is to be brought to the attention of the Head of School immediately and follow the GDPR guidelines for reporting.

Passwords – all staff will be unable to access any device without a unique username and password. Staff passwords will change regularly and if there has been a compromise. IT Support will be responsible for ensuring that passwords are changed. Age appropriate log-ins will be given to children so that they learn the importance of keeping information safe but are still able to access technology with ease.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Services will be responsible for ensuring this task is carried out, and will report to the Head of School if there are any concerns. We do not encourage the use of USB peripherals.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; students upon signing (or parent signing) and returning their acceptance of the Acceptable Use Policy.

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. Emails of a personal nature are not permitted. Similarly, use of personal email addresses for work purposes is not permitted. Staff are expected to communicate with parents in a professional manner (content and tone) and to seek advice from their manager should they have any concerns. All email communication with parents is done through the office rather than being sent directly between the parent and teacher. Further information can be found in the Staff Code of Conduct and Parent Code of Conduct policies. Through our computing curriculum, children discuss the use of emails as communication and learn about how to use them in a safe way. On their school accounts, they do not have access to send or receive emails. Students are taught about respectful use of emails and where they do not follow the acceptable user policy, the use of this software will be withdrawn for a set period of time.

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip upon starting at the school; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; Watchfield Primary School is supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The decision to make these, as well as virtual class display boards, public will be decided by the e-safety officer/Head of School adhering to the guided lines below. Staff are not encouraged to engage in the use of social media within the school community and should be wary of confidentiality and professional boundaries. A broadcast service is a one-way communication method in order to share school information with

the wider school community. No persons will be “followed” or “friended” on these services and as such no two-way communication will take place. In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are “comment enabled”, comments are to be set to “moderated”. All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons). 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.

Monitoring

All staff log behaviour and safeguarding issues related to online safety on CPOMS and this is monitored by the Head of School and DSL. Senior Leaders and Academy Staff may monitor IT use across the school including children and staff use. This policy will be reviewed in accordance with the review cycle. At every review, the policy will be shared with the governing board.

Links to Other Policies

This policy is linked to our:

- Acceptable Use Policy- Staff
- Child protection and safeguarding policy
- Relational Behaviour Policy
- E-Learning Code of Conduct EYFS, KS1 and KS2 (signed by child and parents)
- Staff disciplinary procedures
- Staff Code of Conduct
- Parent Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- Computing policy
- Mobile Phone Policy