Whingate Primary School

Online Safety Policy
October 2026

Date of next review: October 2027

Contents

1. Aims 2
2. Legislation and guidance 3
3. Roles and responsibilities 3
4. Educating pupils about online safety 6
5. Educating parents/carers about online safety 8
6. Cyber-bullying 8
7. Acceptable use of the internet in school 11
8. Pupils using mobile devices in school 12
9. Staff using work devices outside school 12
10. How the school will respond to issues of misuse 13
11. Remote Learning and Working from Home 14
12. Training 14
13. Monitoring arrangements 15
14. Links with other policies 15
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers) 16
Appendix 2: KS2 acceptable use agreement (pupils and parents/carers) 17
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors) 18
Appendix 4: online safety incident log 21
Appendix 5: online safety self audit for staff 22
Appendix 6: Filtering and Monitoring Staff Fact sheet 23

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Co-Headteachers and school staff
- [Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board have overall responsibility for monitoring this policy and holding the Co-Headteachers to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs. The governor who oversees online safety is Ellis Lewis.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Co-Headteachers

The Co-Headteachers are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Co-Headteachers in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Co-Headteachers and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead with SMT on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager (Turn it on group) to make sure the appropriate systems and processes are in place
- Working with the Co-Headteachers, ICT manager (Turn it on group) and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 5 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face with SMT
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager (Turn it on group, Schools Broadband)

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the SMT/DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by speaking to the class teacher, Co-Heads or DSL.
- Following the correct procedures by speaking to class teacher in the first instance or School Business Manager if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'
- Have read the Filtering and Monitoring staff guidance (appendix 6)
- Staff are responsible for their own actions and must act, and be seen to act, in the best interests of children at all times. Staff must ensure they understand and adhere to this guidance as well as Whingate Primary School's code of conduct and Internet Acceptable Use Policy. Staff are responsible for acting promptly to prevent and safeguard children from potential abuse online and for reporting any concerns in accordance with the Leeds Childrens Services Safeguarding & Child Protection Policy for Schools and Colleges.
- Staff are solely responsible for any content on their own personal social media networks and electronic devices. This means that staff are responsible for managing their own applications and content to ensure that it does not breach the school's safer working practice guidance, or undermine public confidence in the school or the education profession. Staff are personally responsible for security and privacy settings when using social media via their chosen equipment and as such failing to ensure adequate and appropriate settings are in place may lead to disciplinary action should the content be found to breach school expectations of professional conduct by bringing the school into disrepute.
- Staff are also responsible for ensuring their own use of ICT and social media is professional and appropriate at all times. Staff must be aware that their conduct online, both inside and outside of school,

must not breach the school's code of conduct or professional expectations. Any behaviour that is deemed to breach such expectations may be subject to disciplinary action.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Co-Headteachers of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

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

Whingate Primary School uses Purple Mash that follows the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage (KS) 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 (KS) 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
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- 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
- How information and data is shared and used online
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online
- That there is a minimum age for joining social media sites, which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

4.2 Pupils will be taught practical cyber security skills

The following items come from the DfE's non-statutory cyber security standards for schools and colleges.

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The physical security of devices
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyber-bullying and the risks of online radicalisation.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety via our website, ClassDojo and email (admin@whingate.com). This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Co-Headteachers and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Co-Headteachers.

6. Cyber-bullying

6.1 Definition

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 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. Class teachers will discuss cyber-bullying with their classes where appropriate or where an issue has arisen.

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 cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers via the website and ClassDojo so 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

All forms of bullying, including cyber bullying, are taken very seriously. Bullying is never tolerated and it is not acceptable for any member of staff to behave in a manner which is intimidating, threatening or in any way

discriminatory. Behaviour which constitutes Bullying or Harassment may be dealt with under the Grievance/Bullying and Harassment Policy and could result in disciplinary action.

However, this doesn't just extend to behaviour within the work place. In some instances bullying or harassment that occurs outside the workplace where there is a link to employment could also fall under the responsibility of the employer and therefore result in disciplinary action being taken against the responsible individual.

Certain activities relating to cyber bullying could be considered criminal offences under a range of different laws. Cyber bullying consists of threats, harassment, embarrassment, humiliation, defamation or impersonation and could take the form of general insults, prejudice based bullying or discrimination through a variety of media. Media used could include email, Virtual Learning Environments, chat rooms, web sites, social networking sites, mobile and fixed-point phones, digital cameras, games and virtual world sites.

If an allegation is received that a member of staff is responsible for comments made online which could be deemed harmful, threatening, defamatory, abusive or harassing in any way towards another employee, the school will investigate this matter. Any allegation of bullying or harassment made by an employee against another member of staff where the accused uses the internet, mobile phone, text message or email, along with any other forms of abuse, may be dealt with through the Grievance/Bullying and Harassment Policy and could lead to disciplinary action.

Staff are required to take steps to protect themselves and their personal information by:

- Keeping all passwords secret and protect access to their online accounts
- Not befriending students and young people on social networking services and sites
- Keeping personal phone numbers private
- Not using personal phones to contact parents and students and young people (unless permission granted by SMT and their number is blocked for instance for Parents' Evening appointments or contacting a parent whilst on residential in the case of an emergency,)
- Keeping personal phones secure, i.e. through use of a pin code.
- Not posting information about themselves that they wouldn't want employers colleagues, students, young people or parents to see
- Not retaliating to any incident
- Keeping evidence of any incident
- Promptly reporting any incident using existing routes for reporting concerns.

Staff in schools, as well as students, may become targets of cyberbullying. Staff should never retaliate to, i.e. personally engage with, cyberbullying incidents. They should report incidents appropriately and seek support.

Staff should report all incidents to the designated line manager or member of their school senior management team. The designated person will take responsibility for ensuring the person being bullied is supported, for investigating and managing the incident, and for contacting the police and Local Authority if appropriate.

For various reasons, staff may find it difficult to report to their line manager in the first instance. They may want additional support or advice. They should know they can seek advice and help from their Union, professional association, from Education Support Partnership, or other organisation.

Further information and advice regarding cyber bullying can be found in the DfE guidance documents Preventing and Tacking Bullying 2017 and Cyberbullying: Advice for Head Teachers and School Staff 2014. https://www.gov.uk/government/publications/preventing-and-tackling-bullying

6.3 Examining electronic devices

The Co-Headteachers, and any member of staff authorised to do so by the Co-Headteachers (as set out in your behaviour policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Co-Headteachers / DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Co-Headteachers, to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / The searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Whingate Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create

images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Whingate Primary School will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school. and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

7.1 Acceptable Use

- To provide communication within the school via email, the school website, text messaging through school or through Class Dojo or Purple Mash messaging facilities
- To provide communication with other schools and organisations for educational purposes
- To distribute details regarding school meetings
- To provide electronic methods of communication
- Any other use that directly supports work related functions

7.2 Unacceptable Use

The following uses will be regarded as not acceptable irrespective of the means of internet access:

- Using the computer to perpetrate any form of fraud, or software, film or music piracy
- Use for racial, sexual, homophobic or other harassment
- To access pornographic, obscene or illegal materialTo solicit personal information with the intent of using such information to cause emotional or physical harm
- Entering into a commitment on behalf of the school (unless you have explicit permission to do this)
- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- Hacking into unauthorised areas
- Publishing defamatory and/or knowingly false material about Whingate Primary School, your colleagues and/or our pupils on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format

- Revealing confidential information in a personal online posting, upload or, transmission, including financial information and information relating to our pupils, staff and/or internal discussions
- Use of personal email to communicate with or about any Whingate Primary School students
- Introducing any form of malicious software into the corporate network
- To disrupt the work of other users, for example, includes the propagation of computer viruses

8. Pupils using mobile devices in school (mobile phones)

The DfE's mobile phone guidance says that the use of mobile phones should be prohibited throughout the school day. At Whingate children in Year 5 and 6 who walk to and from school are permitted to bring their phone. When they arrive at school, they immediately turn it off, hand it to an adult who will put it in a personalised wallet. This is then locked in a stock cupboard for the day. No child is able to access their phone until the adult at the end of the day hands it to them on their way out of the door (not in the cloakroom or classroom).

Mobile phones are not to be taken on any residential by children. Communication to parents/carers will be via ClassDojo.

Pupils will be taught the risks that are associated with the use of mobile phones, both in school and more broadly, to make sure they understand the decision to prohibit the use of mobile phones throughout the school day. These risks can include a loss of focus in lessons, classroom disruption and an increase in bullying. Pupils will be encouraged to see a mobile-phone free environment as desirable and valuable.

8.1 Use of smartwatches by pupils

The DfE's statutory mobile phones guidance includes in the term 'mobile phones' all devices with communications and smart technology that the school chooses to include in its policy.

Smartwatches are wristwatches with smart technology in them. They can be used to tell the time, send and receive text and voice messages, make calls and listen to music. Some smartwatches have wellness and health-related features.

Whingate Primary School do not allow children to wear SMART watches in any circumstance. If a child comes to school with a SMART watch, they will be asked to remove it, locked away and handed back at the end of the day.

9. Staff using work devices outside 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 – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol), or 3 random words
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from School Business Manager, Co-Heads, Turn it on group.

- Staff should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and acceptable use policies which detail how new and emerging technologies may be used.
- Communication with children both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook, Instagram, SnapChat, Whatsapp and X, chat-rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web-cams and other hand-held devices. (Given the ever-changing world of technology it should be noted that this list gives examples only and is not exhaustive.)
- Staff should not have contact with students using social media, and specifically social networking sites without prior permission of the Co-Headteachers. Staff must not add students as friends or respond to friend requests from students. If a member of staff suspects that an existing friend is a student, child or young person, they must take reasonable steps to check the identity of the individual and end the social media friendship.
- It is recognised that personal access to social networking sites outside the work environment is at the discretion of the individual however members of staff should consider their use of social networks as they take on the responsibilities of a professional, taking particular care to secure personal information and ensure their use of such networking sites is respectable and appropriate at all times.
- Members of staff must not take, display or distribute images of students unless they have explicit written consent to do so. Failure to follow any part of this code of practice may result in disciplinary action being taken.

Internet Use

Members of staff must follow and adhere to the policies on the use of IT equipment at all times and must not share logins or password information with other members of staff, students, children or young people, friends, family or members of the public.

As a general principle, internet access is provided to employees to support work related activities. The following list is not intended to be an exhaustive list, but sets out broad areas of use that the school considers to be acceptable uses of the internet.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Remote Learning and Working From Home

Staff working from home can communicate with children during the school day using the year group email address, the email function of Purple Mash, the blog area of Purple Mash, Class Dojo or other sites approved by the School Management Team. Staff can also use the above methods of contact to communicate with children if they are learning remotely.

12. Training

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.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL/deputy DSL, Co-Heads and Assistant Head and all staff 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.

12.1 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

13. Monitoring arrangements

The DSL/Co-Headteachers log behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed every year by the Co-Headteachers. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- KCSIE
- RHSE Policy
- Mobile phone policy
- Social Media policy
- AI policy

Appendix 1:

EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:

When I use the school's devices and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites/apps that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school devices for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Parent/carer agreement: I agree that my child can use the school's devices and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.

Appendix 2

KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy.

When using the school's ICT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break school rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video
- Share my password with others or log in to the school's network using someone else's details
- Create, link to or post any material that is offensive, obscene or otherwise inappropriate
- Bully other people

Pupils may use AI tools:

- That have been approved for their use in school
- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images
- All AI-generated content must be properly attributed and appropriate for the pupils' age and educational needs.

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online
- Mobile phones will be placed in a cupboard throughout the school day (at their own risk) and not removed until the end of the school day.

I understand that school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Parent/carer's agreement: I agree that my child can use the school's devices and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Acceptable use agreement (staff, governors, volunteers and visitors)

Whingate Primary School

Staff Acceptable Use of ICT Agreement / Code of Conduct

1. Acceptable and expected use of ICT.

ICT and the related technologies such as email, the internet and mobile phones are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents and the contents of the ICT Policy, E-safety and Use of Digital Devices and Social Media Guidance. Any concerns or clarification should be discussed with a member of the senior management team.

- I will only use the school's email / Internet / Intranet/One Drive and any related technologies for professional purposes or for uses deemed 'reasonable' by the Co-Headteachers or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role and are made through appropriate channels.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on ARBOR) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not browse, download or upload material that could be considered offensive or illegal. (See examples in 7.2 of the E-safety and Social Media Guidance for Staff.)
- I will not send to pupils or colleagues material that could be considered offensive or illegal.
- Images of pupils will only be taken and used for professional purposes and will not be distributed outside the school network or displayed in a public place without the permission of the parent/ carer.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Co-Headteachers.
- I will respect copyright and intellectual property rights.
- I will support and promote the school's ICT Policy and E-Safety Guidance and Social Media Policy and Online Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I am responsible for the content on my own social media networks and electronic devices and will ensure it does not breach the school's safer working practice guidance or the school's code of conduct and does not undermine public confidence in the school or the education profession;
- I am responsible for the ensuring that adequate and appropriate privacy and security settings are in place when using social media.
- I will not share my personal details such as my home/mobile phone number, social media identities or personal email addresses with students.
- I will not request or accept friend requests from pupils.
- I will not post information which could lead to the identification of someone connected to the school/profession without their explicit consent-this includes images of people.
- I will not install any unauthorised software or connect unauthorized hardware or devices to the school network.
- I will ont promote any private business, unless that business is directly related to the school.

- I will not inappropriately use of AI: Any content produced using AI requires critical judgement to check for appropriateness and accuracy. Whatever tools or resources are used to produce plans, policies or documents, the quality and content of the final document remains the professional responsibility of the person who produced it. Always consider whether AI is the right tool to use. Just because the school has approved its use doesn't mean it will always be appropriate. Always consider whether AI is the right tool to use (Copilot). Just because the school has approved its use doesn't mean it will always be appropriate.

2. The Use of Mobile Phones and SMART watches in School

It is not professional or appropriate for staff to be accessing **mobile phones or SMART** watches whilst performing their duties with children or in the course of their normal work, for example in meetings. Visitors and volunteers are expected to follow the same principles.

Mobile phones and SMART watches must not be used or checked at all:

- By adults when they are working with children, for example:
  -During lesson times.
  -On any corridor or other school space where it would be reasonable to expect that children may be present
  -Whilst supervising children in the classroom, playground, after-school clubs, or on trips.
- By adults when they are performing their normal duties, for example:
  -During staff meetings or briefings.
  -During meetings with colleagues, parents, other professionals.
  -During training sessions in school or other sites.

It is expected practice for phones to be stored away from children, in a teacher's cupboard or similar safe location.

SMART watches will be asked to be removed if staff are found accessing them during learning time, staff meetings or training

Exceptions to this Rule

Phones may be left on and checked in exceptional circumstances and only with the prior agreement of the Senior Management Team, such as:

- When off-site and needing to keep in touch with school.
- When expecting an urgent or important call, such as one regarding a close relative or urgent information, such as relating to medical issues.

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

I agree to follow the *Staff Acceptable Use of ICT Agreement / Code of Conduct,* and have read and understood the ICT Policy, E-safety and Use of Digital Devices a Social Media Guidance to support the safe use of ICT throughout the school.

Full Name: _____

Signature: _____

Date: _____

Appendix 4:

Online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	***Where the incident took place***	***Description of the incident***	***Action taken***	***Name and signature of staff member recording the incident***

Appendix 5: online safety training needs – self-audit for staff

This can be done as a forms questionnaire.

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

Appendix 6

Filtering and Monitoring

Staff Factsheet

Learn about our school's filtering and monitoring systems and how you can help to keep pupils safe online. Know what to do if you have concerns about the content that pupils are accessing.

What is filtering and monitoring?

Filtering systems block access to harmful websites and content.

Monitoring systems:

- Identify when someone searches for or accesses certain types of harmful online content on school devices
- Identify who is searching for or accessing the harmful content
- Alerts the school about it so we can intervene and respond
- **Don't** block access to harmful content

We're all responsible for filtering and monitoring

No filtering and monitoring software is perfect:

- It might not be aware of all the websites that contain inappropriate content
- Abbreviations or misspellings in a search engine may slip past the software
- Inappropriate content may be found on websites considered 'safe'

You can help to make sure the internet is used appropriately by:

- Monitoring what pupils are accessing on devices during school hours (e.g. by looking at their screens when using computers during lessons)
- Alerting Christine Dent if you become aware that content is not being filtered

If you have concerns about what a pupil is accessing online, always raise it with Mell Rose (Designated safeguarding lead (DSL).

Inappropriate content includes:

- Illegal content (e.g. child sexual abuse)
- Discriminatory content (e.g. sexist, racist or homophobic content)
- Sites that promote drugs or substance abuse
- Extremist content (e.g. the promotion of terrorism)

- Gambling sites
- Malware and/or hacking software
- Pornography
- Pirated material (copyright theft)
- Sites that promote self-harm, suicide and/or eating disorders
- Violent material

What systems do we use?

Keeping Children Safe in Education 2023 states that all schools should have appropriate filtering and monitoring systems in place.

We have the following systems in place:

- Whether you are using any particular filtering and monitoring software
  - Schools Broadband set our filters which we have added additional banned words and sites.
  - Filtering checked routinely by school staff and using the SWGfL filtering check, which checks websites on the IWF Child AbuseContent URL list and the Counter-TerrorismInternet Referral Unit list (CTIRU) are blocked and checks that onlinepornography and offensive language is blocked.

- School Response to any filtering and monitoring alerts:
  - Identify user; speak to user and provide support/education if required; implement behaviour policy/disciplinary policy if required and inform parents if required; record incident on monitoring sheet and subsequent actions.
  - Review searched items and identify if filters need to be updated and inform Schools Broadband.
  - If appropriate provide staff feedback through staff briefing.
- Staff responsible for maintenance and review of the software:

  Schools ICT, Christine Dent, Karen Loney, Claire Beswick and Mell Rose

How to raise questions or concerns

Our filtering and monitoring system is designed to protect pupils online. It shouldn't have an impact on teaching and learning or school administration.

Contact: Christine Dent if you and/or pupils:

- Cannot access content that you need to carry out your work
- Have access to content that should be blocked

If you become aware of pupils accessing concerning content at any time, report this Mell Rose as soon as possible.

Sources

This factsheet was produced by The Key Safeguarding: **thekeysupport.com/safeguarding**

Keeping Children Safe in Education, GOV.UK – Department for Education
https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Filtering and monitoring standards for schools and colleges, GOV.UK – Department for Education
https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges

Appropriate filtering, UK Safer Internet Centre
https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-filtering

Appropriate monitoring, UK Safer Internet Centre
https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-