



Waddingham Primary **Online Safety Policy**

This policy was reviewed by the Head Teacher In May 2025 and will be reviewed annually.

Signed Head Teacher:

Date May 2025

Contents

1. Aims.....	3
2. Legislation and guidance.....	3
3. Roles and responsibilities.....	3
4. Educating children about online safety.....	5
5. Educating parents about online safety.....	6
6. Cyber-bullying.....	6
7. Acceptable use of the internet in school.....	7
8. Children using mobile devices in school.....	7
9. Staff using work devices outside school.....	7
10. How the school will respond to issues of misuse.....	7
11. Training.....	8
12. Monitoring arrangements.....	8
13. Links with other policies.....	8
Appendix 1: EYFS and KS1 acceptable use agreement (children and parents/carers).....	9
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (children and parents/carers).....	10
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors).....	11
Appendix 4: online safety training needs – self audit for staff.....	12
Appendix 5: online safety incident report log.....	

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of children, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The four key 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) 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 Head Teachers and school staff](#)
- [Relationships and Health education](#)
- [Searching, screening and confiscation](#)

It also refers to the Department'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 children's 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 has overall responsibility for monitoring this policy and holding the Head Teacher to account for its implementation.

The Governing Board will co-ordinate regular meetings with appropriate staff to discuss online safety, 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;
- Review 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 the Safeguarding Governor

All governors will:

- Ensure that 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 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 Head Teacher

The Head Teacher is 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 DSL and deputy 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:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Undertaking annual risk assessments that consider the risks children face.
- 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 knowledge and skills to safeguard effectively.
- Working with the ICT contractor and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (on CPOMS) and dealt with appropriately in line with this policy
- Working with the Safeguarding Governor to review this policy annually and to ensure the procedures and implementation are updated and reviewed regularly.
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly.
- Working with the ICT contractor to make sure that the appropriate systems and processes are in place.
- 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.
- Responding to safeguarding concerns identified by filtering and monitoring.
-
- 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 3 see attached) 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 Head Teacher and/or Governing Board
- Taking the lead on understanding filtering and monitoring systems and processes in place on school devices and school networks.

This list is not intended to be exhaustive.

3.4 The ICT Provider (Education Lincs)

The ICT contractor is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep children 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 (on CPOMS) 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 children follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (via CPOMS) 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 reports and concerns about sexual violence and/or harassment, both online, and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Head Teacher 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 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 factsheet - [Child net](#)

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.

4. Educating children about online safety

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

From September 2020 **all** schools will have to teach:

- Relationships education and health education in primary schools

This new requirement includes aspects about online safety. As such we've added these expectations in italics below, if your school isn't yet following the RSE 2020 guidance, please remove.

In **Key Stage 1**, children 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

Children 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**, children will know:

- *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 respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*
- *What sorts of boundaries are appropriate in friendships with peers (in all contexts including online) whom they do not know.*

- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*
- *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*
- *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*

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise children's awareness of the dangers that can be encountered online and may also invite speakers to talk to children about this.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

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 and what their children are being asked to do online.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Head Teacher.

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

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 material is illegal. They will also work with external services if it is deemed necessary to do so.

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 children 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.

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 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 report the incident and provide the relevant material to the police as soon as 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.

6.3 Examining electronic devices

The Head Teacher, and any member of staff authorised to do so by the Head Teacher (as set out in the 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 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 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/carers 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 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 [screening, searching and confiscation](#)
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

6.4 Artificial Intelligence

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.

Waddingham 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.

Waddingham 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.

See Artificial Intelligence Policy.

7. Acceptable use of the internet in school

All children, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-2). 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 children, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Children using mobile devices in school

Children may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- During the school day
- Clubs before or after school, or any other activities organised by the school

All phones must be turned off handed into the Class Teachers for safe storage.

Any use of mobile devices in school by children must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a child may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. 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.

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)
- 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

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a child 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 or Governor 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. 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.

11. 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).

The DSL and deputy 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. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. All incidents are recorded on CPOMS as an Online Safety Incident

This policy will be reviewed every year by the DSL. 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.

13. 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
- Artificial Intelligence policy

Appendix 1: Child Acceptable Use Policy

All children must follow this policy when using school technologies and accessing online learning at home.

Children that do not follow this policy may find:

- They have restricted use of technologies in school and when accessing online learning at home.
- An incident report will be logged and reported to parents and the school safeguarding lead.

1	I will only use appropriate language when using the different technologies, including Google Classroom child comment feature.
2	I must not use or create anything that might upset someone or give the school a bad name.
3	I must not give out any personal information (name, address, school, password etc.) – over the Internet.
4	I must not tell my username and passwords to anyone else but my teacher and/or my trusted adults.
5	If I think someone has learned my password then I will tell my teacher and/ or parents/carers.
6	I must never use other people's usernames and passwords or computers left logged in by them.
7	I must log off after I have finished with my computer.
8	I will use the school email system and Google Classroom appropriately as directed by my teacher.
9	I know that everyone has the right to use technologies in school and beyond and I will respect this right.
10	I will report any websites that make me feel uncomfortable to my teacher, or a member of staff or my parent/carers
11	I will tell my teacher, member of staff and/or parents/carers straight away if I am sent any messages that make me feel uncomfortable.
12	If I find something that I think I should not be able to see, I must tell my teacher and /or parents/carers straight away and not show it to other children.
13	I will be kind to others and not upset or be rude to them

Child User Agreement Form for the Acceptable Use Policy

My teacher has explained the rules of acceptable use of technologies in school, including online learning at home and I agree to follow them.

I agree to report anyone who is not following the school policy to my teacher.

If I do not follow the rules I may have restricted use of technologies in school and be removed from the online learning platform.

Name _____ Class: _____

Child's Signature: _____

Parent/Carers/Signature: _____

Date: _____

Appendix 2



Appendix 3: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT

Name of staff member/volunteer:	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?	
Do you know what you must do if a child approaches you with a concern or issue?	
Are you aware of the ways pupils can abuse their peers online?	
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?	
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 children and parents?	
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?	