eSafety Policy

Waddesdon Village Primary School – *a Pathway to Excellence*

Approved by:	Laura Forchione	**Date:**	February 2026
Last reviewed on:	February 2026		
Next review due by:	February 2027		

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, 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

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and 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 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 body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs and records and analysis of filtering and monitoring as provided by the designated safeguarding lead (DSL).

A governor is appointed to oversee online safety.

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 2)

3.2 The headteacher

The headteacher 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

Details of the school's designated safeguarding lead (DSL) and deputy are set out in our child protection and safeguarding policy.

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

- In ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that effective monitoring strategies are in place to meet safeguarding needs
- Ensuring that any filtering and monitoring incidents are logged (see appendix 5) and dealt with in line with this policy
- Review filtering and monitoring provision at least annually
- 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 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 governing body

This list is not intended to be exhaustive.

3.4 ICT Management (JSL, Senior Leadership Team and Computing Co-ordinator)

The managers are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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

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 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and any filtering and monitoring issues are logged (see appendix 5) 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

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher 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 (appendix 1).

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

- https://nationalcollege.com/enrol/waddesdon-village-primary-school
- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

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 2).

4. Educating pupils about online safety

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

Lessons will be based on the 8 topics outlined in the UKCIS Education for a Connected World Framework

- Self-image & identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information

- Health, wellbeing & lifestyle
- Privacy & security
- Copyright & ownership

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

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 pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

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 or during parents' evenings. This policy will also be shared with parents.

Parents will be invited to sign up to https://nationalcollege.com/enrol/waddesdon-village-primary-school where a range of guides and advice is available.

Parents will be reminded, at least annually, that photographs and videos taken at sports days, performances and assemblies etc. should be for their personal use only and advised to avoid posting images of other families' children on social media without consent.

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

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

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.)

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 in 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, citizenship and economic (PSHCE) 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).

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.

6.3 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.

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 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

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

7. Acceptable use of the internet in school

All parents (having discussed with children), 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 and 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 pupils, 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. Pupils using mobile devices in school

Children are not permitted to bring mobile phones, tablets or laptops onto the school site. In certain circumstances, the head teacher may grant permission if it is in the best interest of the child/family. In these cases, the device will need to be handed in to the school office upon arrival at school and collected at the end of the school day. The device may not be turned on whilst on the school grounds.

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, as set out in appendix 2.

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. USB devices may not be used in school devices.

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 pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. 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. 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 filtering and monitoring, 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).

All staff will undertake child protection and safeguarding training, which will include online safety, annually. They will also update their knowledge and skills on the subject of online safety at least every two years.

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. Filtering and Monitoring arrangements

Filtering and monitoring systems are used to keep pupils safe when using the school's IT system.

All staff log behaviour and safeguarding issues relating to online safety on the incident report log appendix 4 and filtering and monitoring issues on appendix 5.

These are then passed immediately to the DSL.

The DSL reviews and actions issues relating to online safety raised on appendix 4 and filtering and monitoring raised on appendix 5.

This policy will be reviewed annually by the Computer co-ordinator. At every review, the policy will be shared with the governing board.

13. Use of Artificial Intelligence Tools

Our Generative AI policy sets out how school staff may make use of AI tools in the course of their duties. It is the school's policy that no pupils will be given access to commercial AI tools during the school day and access to these is blocked by the school's filtering and monitoring service.

The computing scheme of work that we follow, Purple Mash, includes limited use of AI as part of specific lessons. The tools used are part of the 2Simple platform and will be monitored in the same way as all other aspects of pupils' ICT usage.

If parents have any concerns about their children's use of AI tools outside of school then these should be raised in the first instance with the headteacher and/or DSL as usual.

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
- Computing Policy
- Social Media Policy
- Use of Generative AI Policy

Appendix 1: 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 using the school's ICT systems 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
- 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 my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

I will not bring a personal mobile phone or other personal electronic device into school unless I have had permission from the head teacher. If am I authorized to bring in a device:

- I will hand it to the office upon arrival at school.
- I will collect it from the office at the end of the school day and ensure it is not turned on whilst on the ground grounds.

I agree that the school will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

Child/Parent/carer agreement:

I confirm that I have discussed this agreement in full with my child and they agree to these points.

I agree that my child can use the school's ICT systems 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.

Signed ():	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms (This can be done on personal devices, using the school's guest wifi, outside of lesson times).
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Use any USB devices in any school equipment
- Open files brought in on removable media (CD's, etc.) until they have been checked and authorised.
- Share my password with others or log in to the school's network using someone else's details

When accessing my school email via a non-school device, such as a personal mobile phone or tablet, I will only do so via an internet browser to ensure that I need to use my email password every time. I will not set up school emails to come automatically to my phone or use the office365 app for school emails.

When sending a sensitive email that contains personally identifiable information, include the word 'encrypt' within the subject field to encrypt the email you are sending.

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit.

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.

Signed (staff member/governor/volunteer/visitor):	**Date:**

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

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
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 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?	
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? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 5: Records and analysis of filtering and monitoring 1/2

Records and analysis of filtering and monitoring.

REPORT FORM

Name of School	Waddesdon Village Primary School
School Number	8252317
Name(s) of child and year group	
Date reported	
Date of incident	
Reported to	
Reported by	

Description of the incident:
Any other relevant information (context of information shared, witnesses, immediate action taken):

Incident involves the following:

Illegal	Child abuse images and terrorist content.	
Bullying	Involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others.	
Child Sexual Exploitation	Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet.	
Discrimination	Promotes the unjust or prejudicial treatment of people with protected characteristics listed in the Equality Act 2010.	
Drugs / Substance	Abuse displays or promotes the illegal use of drugs or substances.	
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance.	
Gambling	Enables gambling.	
Pornography	Displays sexual acts or explicit images.	
Self-Harm	Promotes or displays deliberate self-harm.	
Violence	Displays or promotes the use of physical force intended to hurt or kill.	
Suicide	Suggest the user is considering suicide.	
Other – please record:		

Appendix 5: Records and analysis of filtering and monitoring 2/2

Action taken by staff member: **Reporting staff signature …….. Date ……..…** **Passed to DSL ……Time/date ……**
Action taken by Designated Safeguarding Lead: **Response/outcome:** **DSL signature ……. Date ……**