



The Horsell Village School

E Safety Policy

School Name: The Horsell Village School
Date: Autumn 2026
Date shared with LGC: Autumn 2026
Date shared with staff: Autumn 2026

Rationale

Technology and the internet are an important part of children's learning and development. The Horsell Village School uses digital technology to enhance teaching and learning and to provide children with opportunities to develop the knowledge, skills and confidence they need to participate safely in an increasingly digital world.

Children at The Horsell Village School regularly use school-owned iPads to support their learning. These devices provide access to educational applications, websites and other digital resources selected or approved by the school.

Our Online Safety Policy has been developed in line with current government guidance and good practice. It forms part of our wider safeguarding arrangements and should be read alongside the school's Child Protection and Safeguarding Policy, Computing Policy, Behaviour Policy, Data Protection Policy, Staff Acceptable Use Policy, Mobile Phone Policy and other relevant policies.

As an infant school, our approach to online safety recognises the age and developmental stage of our children. Children in Reception, Year 1 and Year 2 require appropriate adult guidance and supervision when using technology and accessing online content. Our aim is therefore not simply to restrict access, but to teach children safe and responsible behaviours from an early age.

Online safety is a safeguarding matter and is the responsibility of the whole school community. Staff, governors, parents/carers and children all have an important role to play in helping children develop safe and positive digital habits.

Our vision for online safety

The Horsell Village School aims to provide a safe, positive and purposeful environment in which children can benefit from technology.

We aim to:

- provide children with meaningful and age-appropriate opportunities to use technology as part of their learning;
- teach children how to use technology safely, responsibly and respectfully;
- help children recognise when something online is inappropriate, upsetting or makes them feel uncomfortable;
- teach children to stop, close the device or screen and tell a trusted adult if they see something that worries them;
- ensure that children's access to online content is appropriately filtered, monitored and supervised;
- balance appropriate safeguarding measures with the educational benefits of technology;
- support staff to use technology safely and professionally;
- work in partnership with parents and carers to promote safe use of technology at home as well as at school;
- respond promptly and appropriately to online safety concerns and incidents.

Online safety education will reflect the age and developmental needs of our pupils and will be embedded within Computing and the wider curriculum.

Using this policy

This policy applies to the use of technology and digital communication by members of the school community.

This includes, but is not limited to:

- school-owned iPads and other tablets;
- computers and laptops;
- interactive displays;
- the school's network and internet connection;
- educational applications and online learning platforms;
- websites and online resources;
- email and other school-approved communication systems;
- video and audio resources;
- cameras and microphones;
- school websites and social media;
- personal devices when they are being used on school premises or for school business.

The policy applies to technology used in school and, where relevant, to online activity outside school which has a safeguarding or significant impact on members of the school community.

Roles and responsibilities

Online safety is a shared responsibility. All members of the school community have a role in maintaining a safe digital environment.

Headteacher and Senior Leadership Team

The Headteacher and Senior Leadership Team are responsible for:

- ensuring that online safety forms part of the school's safeguarding arrangements;
- ensuring that this policy is implemented and reviewed;
- ensuring that appropriate filtering and monitoring arrangements are in place;
- ensuring that staff receive appropriate online safety training;
- ensuring that online safety concerns are appropriately recorded, investigated and acted upon;
- working with the school's IT support/provider to address technical concerns;
- ensuring that governors are appropriately informed about online safety arrangements and significant concerns.

Designated Safeguarding Lead

The Designated Safeguarding Lead (DSL) has responsibility for responding to online safety concerns where there is a safeguarding element.

The DSL will:

- respond to online safety concerns in accordance with the school's safeguarding procedures;
- ensure that safeguarding concerns are appropriately recorded;
- liaise with parents/carers and external agencies where appropriate;
- ensure that online safety concerns are considered alongside wider safeguarding information about a child;
- work with the Online Safety Leads and IT support where technical or educational action is required.

The Online Safety Leads and DSL(s) will work together where an online safety concern has a safeguarding element.

Online Safety Leads

Emma Jarvis and Jane Reeve are responsible for leading online safety across the school.

They will:

- act as points of contact for online safety matters;
- support the development and review of the school's Online Safety Policy;
- keep up to date with relevant online safety guidance and developments;
- support staff in promoting safe and responsible use of technology;
- support the embedding of online safety within Computing and the wider curriculum;
- work with the DSL where an online safety concern has a safeguarding element;
- liaise with IT support regarding technical online safety concerns;
- support the review of filtering and monitoring arrangements;
- support staff training and awareness;
- monitor online safety incidents and identify any patterns or emerging concerns;
- promote online safety to parents and carers.

The Online Safety Leads are not responsible for replacing or undertaking the role of the DSL. Safeguarding concerns will always be managed in accordance with the school's Child Protection and Safeguarding Policy.

All staff

All staff are responsible for:

- following this Online Safety Policy and the school's Acceptable Use Policy;
- modelling safe, responsible and respectful use of technology;
- supervising children's use of iPads and other technology appropriately;
- using only school-approved accounts, applications and resources;
- reporting online safety concerns promptly;
- reporting inappropriate or unexpected content encountered on school devices;
- maintaining professional boundaries when using digital communication;
- protecting passwords and confidential information;
- completing relevant online safety training.

Managing access and security

The school will provide children with managed and appropriately filtered access to the internet. Children's access will be appropriate to their age and developmental stage.

In particular:

- Internet access will normally take place through school-managed iPads or other school equipment.
- Children will access the internet primarily for educational purposes.
- Staff will select or direct children towards appropriate websites, applications and online resources.
- Children's internet use will be appropriately supervised.
- Filtering and monitoring systems will be used to reduce children's exposure to harmful or inappropriate content.

School devices will be managed and maintained securely.

Access to school systems will be controlled through appropriate authentication and account-management arrangements.

Passwords and login information must be kept confidential.

Staff must not share their passwords with children.

School devices must not be used to access inappropriate or unauthorised content.

Any concern about filtering, monitoring or inappropriate content must be reported to the appropriate member of staff.

The school recognises that no filtering system can guarantee that inappropriate content will never be accessed. Filtering and monitoring are important safeguards but do not replace appropriate supervision, education and professional judgement.

The school will review its filtering and monitoring arrangements regularly and work with its IT provider where concerns are identified.

Children's use of iPads

School-owned iPads are provided to support children's learning.

Children are expected to:

- use iPads carefully and responsibly;
- use only the applications, websites and resources directed or approved by a member of staff;
- remain on the activity they have been asked to complete;
- not attempt to change settings or security controls;
- not attempt to access websites, applications or content that they have not been directed to use;
- not use another person's account;
- not share passwords or login information;
- ask an adult for help if they are unsure what to do;
- tell an adult immediately if they see something that worries, upsets or confuses them.

Children will be taught a simple, age-appropriate response to unexpected or worrying content:

STOP – CLOSE – TELL

STOP what you are doing.

CLOSE the website, app or screen if it is safe to do so.

TELL a trusted adult.

Children will not be expected to investigate, delete or manage an online safety incident themselves.

Online safety education

Online safety education will be embedded within Computing and the wider curriculum and will be appropriate to the age and developmental stage of the children.

Children will be taught, in an age-appropriate way, about:

- safe and responsible use of technology;
- keeping personal information private;
- recognising trusted adults;
- asking for help when something online worries them;
- recognising appropriate and inappropriate content;
- respectful behaviour when using technology;
- being kind and considerate online;
- safe use of photographs, cameras and microphones;
- keeping passwords and other information secure;
- recognising that not everything they see or hear online is necessarily true;
- understanding that people online may not always be who they say they are;
- balancing screen use with other activities;
- the importance of telling an adult about something that makes them feel uncomfortable.

For our youngest children, online safety education will be delivered through practical activities, stories, discussion, modelling and age-appropriate scenarios rather than relying solely on written rules.

Teaching and learning

Technology will be used where it provides a clear educational benefit.

Teachers will:

- plan appropriate learning activities involving technology;
- select suitable websites, apps and digital resources;
- consider the age and needs of the children before using an online resource;
- provide clear instructions and expectations;
- supervise children appropriately;
- consider accessibility and individual children's needs;
- respond appropriately if children encounter unexpected or inappropriate content.

Children will generally use a limited range of school-approved websites, applications and digital resources rather than being expected to navigate the wider internet independently.

Where children undertake online research, staff will provide appropriate guidance and support.

At this age, children will not normally be expected to independently assess the reliability of a wide range of online sources.

Copyright and the responsible use of digital content will be introduced in an age-appropriate manner.

Email and online communication

Children in Reception, Year 1 and Year 2 will not normally use email or online messaging independently.

Where online communication is required for an educational activity:

- it will be organised and supervised by a member of staff;
- school-approved accounts or platforms will be used;
- children will not communicate privately with unknown individuals;
- children will not be permitted to use personal email or messaging accounts on school devices;
- staff will follow the school's safeguarding and data protection procedures when communicating electronically.

All communication between staff and children or families will take place using school-approved systems and accounts.

Video calls and live online activities

Any video call or live online activity involving children must be:
approved by the school;

- undertaken using a school-approved platform;
- organised by a member of staff;
- appropriately supervised;
- planned with consideration of safeguarding and privacy;
- communicated to parents/carers where appropriate.

Children will not independently make or receive video calls using school devices.

Social media and online platforms

Children will not be permitted to access social networking platforms through school devices unless a specific platform has been approved by the school for an educational purpose.

Children will not be expected to maintain personal social media accounts as part of their learning.

Any school social media accounts will be managed by authorised staff in accordance with the school's Social Media Policy.

Staff must maintain appropriate professional boundaries when using social media and must not communicate with children through personal social media accounts.

Video and multimedia content

Online video and multimedia resources can provide valuable learning opportunities but can also contain inappropriate or unexpected content.

Staff must:

- use school-approved or appropriately reviewed resources wherever possible;
- check videos and other online content before showing them to children;
- consider the age suitability of content;
- consider adverts, comments, recommendations and other content that may appear alongside a resource;
- avoid exposing children to unmoderated content where there is a foreseeable risk of inappropriate material;
- report any inappropriate content encountered.

Where there is uncertainty about whether a resource is appropriate, staff should seek advice from the Online Safety Leads, DSL or SLT before using it.

Cameras, photographs and recordings

School devices may include cameras and microphones and these will only be used for legitimate educational or school purposes.

Children will be taught that:

- they should ask permission before taking photographs or recordings of other people;
- they should not take photographs or recordings of people without permission;
- photographs and recordings should be used only for the intended purpose;
- they should tell an adult if they are unsure whether it is appropriate to take a photograph or recording.

Staff must follow the school's Data Protection Policy and procedures when taking, storing or sharing photographs, videos or recordings of children.

Publishing children's images and work

The school may publish photographs, videos or examples of children's work for appropriate educational and promotional purposes where appropriate consent has been obtained.

The school will:

- follow its data protection and image consent procedures;
- avoid publishing unnecessary personal information;
- use only school-controlled websites and social media accounts;
- ensure published content is appropriate and respectful;
- consider the safeguarding implications of publishing children's images and work.

Parents/carers will be provided with information about the school's approach to the use of children's images and will be able to provide or withdraw consent in accordance with the school's procedures.

Personal devices

School staff should use school equipment wherever possible for school business.

Where personal devices are permitted for school purposes, staff must follow the Staff Acceptable Use Policy and Data Protection Policy.

Staff must not:

- store children's photographs or personal information unnecessarily on personal devices;
- use personal messaging or social media accounts to communicate with children;
- allow children to access personal devices;
- use personal devices in a way that breaches professional boundaries or school policies.

Mobile phones

Children are not normally permitted to use mobile phones during the school day.

If a child needs to bring a mobile phone to school because of particular circumstances, this must be agreed with the school in advance. The phone should be stored securely and should not be accessible to the child during the school day.

Staff mobile phones must not be accessible to children and should not be used for taking photographs or recordings of children.

The school will follow its separate Mobile Phone Policy where applicable.

Personal data and privacy

The school recognises that online safety and data protection are closely connected.

The school will follow its Data Protection Policy and relevant data protection legislation.

Staff and children will be taught, at an appropriate level, about protecting personal information.

Children will be encouraged not to share information such as:

- their full name;
- home address;
- telephone number;
- passwords;
- photographs without permission;
- information about themselves or others that could put someone at risk.

The school will ensure that personal data is handled securely and only shared where there is an appropriate lawful basis.

Artificial intelligence and emerging technologies

The school recognises that artificial intelligence and other emerging technologies are increasingly becoming part of children's lives.

Any use of AI tools within school will be considered carefully by the school before being introduced.

The school will consider:

- age appropriateness;
- safeguarding risks;
- privacy and data protection;
- accuracy and reliability;
- whether the tool is appropriate for the intended learning purpose;
- whether children could encounter inappropriate or harmful content;
- whether the service meets relevant school and DfE expectations.

Children in EYFS and Key Stage 1 will not be expected to use generative AI tools independently.

Authorising access

All staff and other authorised users must comply with the school's relevant Acceptable Use Policy before, SLT and IT support/provider to review reviewed annually, or sooner where there are

significant changes to legislation, government guidance, technology, the school's accessing school IT systems.

Children will be taught the school's age-appropriate expectations for safe technology use.

Children's access to the internet will normally be:

- directed by a member of staff;
- supervised appropriately;
- through school-managed devices;
- limited to educationally appropriate resources;
- subject to the school's filtering and monitoring arrangements.

•

Parents/carers will be informed about the school's approach to children's use of technology and online safety.

Assessing and managing risk

The school recognises that online risks can include:

- exposure to inappropriate or harmful content;
- contact with inappropriate individuals;
- sharing of personal information;
- inappropriate communication;
- cyberbullying;
- misuse of images;
- online scams and fraudulent content;
- misinformation;
- excessive or inappropriate use of technology;
- risks associated with emerging technologies.
- The school will take reasonable and proportionate steps to minimise these risks through:
 - appropriate filtering;
 - monitoring;
 - supervision;
 - staff training;
 - age-appropriate online safety education;
 - careful selection of digital resources;
 - appropriate device and account management;
 - clear reporting procedures.

The school will consider the age of its pupils and the level of access they have to IT systems when assessing online safety risks.

Responding to inappropriate content

If a child encounters inappropriate, harmful or upsetting content:

- The child should tell a trusted adult.
- The member of staff should respond calmly and reassure the child.
- The child should not be blamed or made to feel that they have done something wrong.
- The device or content should be left available where appropriate so that the incident can be investigated.
- The member of staff should report the incident in accordance with school procedures.
- The DSL should be informed if there is a safeguarding concern.
- Technical concerns should be reported to the appropriate IT support/provider.
- Parents/carers will be informed where appropriate and in accordance with safeguarding procedures.

- Staff should not investigate safeguarding concerns beyond their role or attempt to resolve potentially harmful content themselves. The school's safeguarding procedures should be followed.
- Where inappropriate content has been accessed because of a filtering failure, the incident should also be reported to the Online Safety Leads so that the school's technical arrangements can be reviewed.

Online safety incidents and complaints

Online safety concerns will be taken seriously and dealt with promptly.

Concerns may be reported by:

- children;
- parents/carers;
- staff;
- governors;
- visitors;
- other members of the school community.

Concerns involving potential harm to a child will be dealt with under the school's safeguarding procedures.

Concerns relating to behaviour or misuse of technology will be dealt with in accordance with the school's Behaviour Policy and relevant Acceptable Use Policy.

Significant online safety incidents will be recorded appropriately so that the school can identify patterns, review practice and take preventative action.

Misuse of technology

The school will respond to misuse of technology in an age-appropriate and proportionate way.

For young children, this will normally focus on:

- explaining why the behaviour is unsafe or inappropriate;
- helping the child understand what they should do instead;
- reinforcing safe use of technology;
- involving parents/carers where appropriate;
- considering whether further safeguarding or pastoral support is required.

Where staff misuse technology, the matter will be dealt with under the school's staff procedures and relevant policies.

Serious or persistent misuse may require further action in accordance with the school's Behaviour, Safeguarding or Staff Disciplinary procedures, as appropriate.

Parents and carers

The school recognises that children use technology outside school and that parents and carers play an important role in helping children develop safe online habits.

The school will:

- provide parents/carers with information about online safety;
- share advice and resources where appropriate;
- raise awareness of emerging online risks;
- encourage parents/carers to talk to their children about their online experiences;
- encourage children to tell a trusted adult if something online worries them;
- work with families when online safety concerns arise.

Parents/carers are encouraged to supervise children's use of technology at home and to use appropriate parental controls and age restrictions.

Monitoring, review and evaluation

The school will review its online safety arrangements regularly.

This will include consideration of:

- online safety incidents;
- filtering and monitoring reports;
- staff and pupil feedback;
- emerging technologies and risks;
- changes to government guidance;
- the effectiveness of online safety education;
- the needs and age profile of the children;
- the effectiveness of technical safeguards.

The school's filtering and monitoring provision will be reviewed at least annually and following significant changes to the school's technology or safeguarding arrangements.

The Online Safety Leads will work with the DSL, SLT and IT support/provider to review any significant incidents or emerging patterns.

The policy will be updated when required to reflect changes in technology, legislation, guidance or the school's circumstances.

Related policies and documents

This policy should be read alongside:

- Child Protection and Safeguarding Policy
- Staff Acceptable Use Policy
- Pupil/Parent Acceptable Use Agreement
- Behaviour and Relationships Policy
- Data Protection Policy
- Social Media Policy
- Mobile Phone Policy
- Staff Code of Conduct
- Computing Policy
- Complaints Policy
- Anti-Bullying Policy