Cherry Orchard Primary School

"We care, we learn, we succeed"

Cherry Orchard Online Safety and Acceptable Use Policy

Date of Policy: September 2026
Member of Staff Responsible: Online safety DSL (Emma Emery)
Review Date: September 2027

To be read in conjunction with the Safeguarding and Children Protection Policy, Anti-Bullying Policy, RHE Policy, Staff code of Conduct, Data Protection Policy, Staff Disciplinary Policy and Procedures, Pupil Remote Learning Policy, Prevent Risk Assessment, Mobile Phone and Wearable Technologies Policy, and the Behaviour Policy.

Ethos Statement

At Cherry Orchard Primary School we are committed to creating a safe learning environment for pupils to learn. We readily use a range of technologies to deliver the curriculum and enhance pupils' experiences during the school day and at home. We expect all members of our school community to follow our Online Safety Policy.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- Content – being exposed to illegal, inappropriate or harmful material
- Contact – being subjected to harmful online interaction with other users
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm
- Commerce – exploitation through online marketing suc as on apps and games websites.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Aims

We aim to help every pupil and adult to:

- Feel safe and confident when using new technologies
- Know who to speak to if they feel unsafe
- Know how to report any abusive behaviour
- Know how to use the internet correctly, without misuse
- Stay in control and keep personal information private.

Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The General Data Protection Regulation (GDPR)
- DfE (2026) 'Keeping children safe in education'
- DfE's 'Relationships and sex education and health education' statutory guidance 2026
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

Roles and Responsibilities

All the adults that are involved in the life of the school, whether governors, teaching staff, support staff, technicians and the community, have roles and responsibilities that are associating with online safety as well as all pupils that come into contact with computers.

Governors

The governing body is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance
- Ensuring the DSL's remit covers online safety
- Reviewing this policy on an annual basis
- Ensuring their own knowledge of online safety issues is up-to-date
- Ensuring all staff undergo safeguarding and child protection training (including online safety) at induction
- Ensuring that there are appropriate filtering and monitoring systems in place and are reviewed annually.

Head Teacher and Senior Leadership

The headteacher and Senior Leadership team are responsible for:

- Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training
- Ensuring online safety practices are audited and evaluated
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety

- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe
- Working with the DSL and governing board to update this policy on an annual basis.

Teaching and Support Staff

Teaching and Support Staff are responsible for:

- Ensuring they stay up to date with current online safety matters, policies and practice
- Reading, understanding and carrying out the Acceptable Use Policy and online safety and signing to say that they have read the policy
- Reporting any misuse or problems to the Head Teacher, Online Safety Lead (Emma Emery) or another DSL for further investigation
- Ensuring any digital communications with pupils is strictly professional and only carried out using school systems
- Ensuring online safety issues are embedded throughout the curriculum
- Ensuring pupils follow the Online Safety policy
- Awareness of online issues related to the use of mobile phones, cameras and hand held devices and monitoring their use and implementing current school policies with regards to these devices
- Modelling good online behaviours
- Having an awareness of online safety issues.

Designated Safeguarding Leaders

The lead DSL for Online safety is Emma Emery.

The lead DSL as well as other DSLs are responsible for:

- Taking the lead responsibility for online safety in the school
- Acting as the named point of contact within the school on all online safeguarding issues
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online
- Liaising with relevant members of staff on online safety matters, e.g. the Inclusion Leader and IT technician
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented
- Ensuring safeguarding is considered in the school's approach to remote learning
- Ensuring appropriate referrals are made to external agencies, as required

- Staying up-to-date with current research, legislation and online trends
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff
- Ensuring all members of the school community understand the reporting procedure
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures
- Working with the headteacher and governing board to update this policy on an annual basis.

IT technician is responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures
- Implementing appropriate security measures as directed by the headteacher or SLT
- Ensuring that the school's filtering and monitoring systems are reviewed and updated as appropriate

Pupils

Pupils and students are responsible for:

- Knowing and acting accordingly to the school's Online Safety and Acceptable Use Policy
- Knowing the importance of reporting abuse, misuse or access to inappropriate materials and know how to report them
- Knowing the policy on mobile phones, digital cameras and other hand held devices and to realise these can be used for cyber-bullying
- Understanding that the Online Safety policy also covers their actions out of school, if related to their membership of the school.

SMART Rules

Pupils should be aware of the 5 SMART rules which are published by Childnet International:

S - Safe: Keep safe by being careful not to give out personal information such as your name, email address, home address, school name, phone numbers and photographs.

M - Meeting: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parent's or carer's consent and only when they can be present.

A - Accepting: Accepting emails, instant messages, files or texts from strangers can lead to safeguarding concerns.

R - Reliable: Information you find on the internet may not be true, or someone online may be lying about who they are.

T - Tell: Tell your parent, carer or trusted adult if someone or something makes you feel uncomfortable or worried or if someone you know is being bullied online. 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.

Parents/ Carers

Parents and carers have the responsibility to ensure that their children use the internet and mobile phones correctly and do not misuse these technologies. They must be aware of the school's Online Safety Policy.

Other Users

Volunteers, including governors, who help in the school and who use information and communication technology systems and devices in helping the school are expected to:

- Use information and communication technology in accordance with this policy and the training provided
- Report any suspected misuse or problem to the person designated by the school for this purpose.

Educating Pupils about Online Safety

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- PSHE including RHE (updated 2026)
- Computing

The curriculum and the school's approach to online safety is developed in line with the UK Council for Internet Safety's 'Education for a Connected World' June 2020 framework and the DfE's 'Relationships and sex education and health education' statutory guidance 2026.

The curriculum will focus on two areas: online relationships and internet safety and harms.

Online Relationships

By the end of their education at Cherry Orchard, pupils will know:

- The nature of online spaces: That people sometimes behave differently online, including pretending to be someone they are not.
- Online friendships: That the same principles of positive, respectful friendships apply online as they do in person (including respect for anonymity and privacy).

- Information sharing: The risks involved with sharing information and images online, and how information can be shared widely or stored indefinitely.
- Critical consumption: How to critically evaluate what they see online, including recognizing that not all information is true or safe.

Internet Safety and Harms

By the end of their education at Cherry Orchard, pupils will know:

- Digital footprint & tracking: That their online actions leave a digital footprint and that data is generated and used by companies.
- Screen time balance: How to identify the benefits of rationing time spent online and the importance of balancing online time with offline activities.
- Recognising harm: How to spot internet-based harms, including cyberbullying, age-inappropriate content, and online manipulation including 'deep fakes'.
- Reporting and help-seeking: Where and how to report issues, seek help, and flag up worries or unsafe experiences (e.g., to a teacher, parent, or trusted adult).

The online risks pupils may face online are always considered when developing the curriculum. The DSL is involved with the development of the school's online safety curriculum.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the Inclusion leader and designated teacher for LAC, and the DSL for online safety work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.

Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a record on CPOMS so that the DSLs are informed.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the safeguarding reporting procedures.

Remote learning

All remote learning is delivered in line with the school's Remote Learning Policy.

Artificial Intelligence (AI) and Digital Literacy

The school recognises that Artificial Intelligence (AI) is an evolving part of the digital world, presenting both educational opportunities and unique risks such as misinformation, deepfakes, and data privacy concerns. We proactively manage these risks through a spiral curriculum that builds pupils' critical thinking and digital literacy, teaching them how to question the authenticity of online content and use technology ethically. This classroom learning is strictly balanced with **robust technical filtering, clear Acceptable Use Policies (AUPs), and vigilant staff oversight** to ensure a safe, age-appropriate learning environment.

Staff use of AI

Microsoft Copilot is used as a tool to reduce teacher workload and support high-quality teaching supported by CPD and recommendations in the EEF guidance report, 'Using digital technology to improve learning'. Teachers will always check the accuracy and suitability of resources produced by AI before using them in the classroom. In the case of intellectual property (e.g. uploading pupils' work for marking and feedback), consent must be obtained from parents and carers.

Cyber-Bullying (child on child abuse)

Cyber-bullying is bullying that takes place online, including through social media, messaging apps, websites and gaming platforms.

Like all forms of bullying, it involves:

- Deliberate and repeated behaviour intended to cause harm
- An imbalance of power between those involved
- Emotional, social or psychological harm to an individual or group.

  (See also the Behaviour Policy and Anti-Bullying Policy.)

Preventing and Responding to Cyber-Bullying

Prevention

The school will:

- Teach pupils what cyber-bullying (online bullying) is, how to recognise it and how to report concerns.
- Encourage pupils to report incidents whether they are a victim or a witness.
- Discuss cyber-bullying regularly through:
    - PSHE/RHE education
    - Computing lessons
    - Other curriculum opportunities
    - Assemblies
    - Class discussions
- Provide safeguarding training for staff, governors and volunteers on cyber-bullying and online safety.
- Share information and guidance with parents about recognising, reporting and supporting children affected by cyber-bullying.

Responding to Incidents

When cyber-bullying occurs, the school will:

- Take reasonable steps to contain the incident and minimise further harm
- Work with external agencies where appropriate
- Report illegal content or activity to the police when there are reasonable grounds to believe an offence has been committed.

The Designated Safeguarding Lead (DSL) will coordinate any safeguarding response and liaise with the police and other relevant agencies where necessary.

Examining Electronic Devices

School staff have legal powers under the Education and Inspections Act 2006 and the Education Act 2011 to search and, where appropriate, delete files or images on a pupil's electronic device.

Devices may be searched if they:

- Pose a risk to staff or pupils
- Are identified in school rules as prohibited items
- May contain evidence relating to an offence.

Data or files may be examined if staff reasonably suspect they have been used to:

- Cause harm
- Undermine the safe environment of the school
- Disrupt teaching and learning
- Commit an offence.

Handling Inappropriate Material

Where inappropriate material is found:

- Staff will consult with the DSL or a senior leader to determine the appropriate response
- Safeguarding concerns will always be prioritised
- Material that may be evidence of a crime will not be deleted and the device will be passed to the police as soon as practicable
- Material may be deleted if:
    - It is likely to cause harm if retained; and/or
    - The pupil or parent refuses to remove it themselves.

Suspected Indecent Images of Children

If staff suspect a device contains a nude or semi-nude image of a child, they will:

- Not view the image.
- Confiscate the device.
- Immediately report the matter to the DSL.

  The DSL will follow current DfE guidance on searching, screening and confiscation, together with UKCIS guidance on sharing nude and semi-nude images.

Complaints

Any complaints regarding searches or deletion of material from electronic devices will be managed through the school's Complaints Procedure.

Staff Use of Work Devices Outside School

All staff must comply with:

- The Acceptable Use Agreement for ICT Systems and Internet
- The Safeguarding and Child Protection Policy
- Data Protection Policy

Failure to comply may result in disciplinary action.

Security Requirements

When working remotely, staff must:

- Keep devices secure and password protected
- Take reasonable steps to prevent unauthorised access
- Seek advice from the ICT provider if they have concerns about device security

- Use work devices solely for work-related purposes.

Staff Must:

- Use strong passwords (minimum 8 characters including upper and lower-case letters, numbers and special characters)
- Ensure devices automatically lock when left inactive
- Not share school devices with family members or friends
- Follow all school acceptable use requirements.

IT Support

The school's ICT provider will:

- Install and maintain anti-virus and anti-spyware software
- Ensure operating systems are kept up to date.

Data Protection

- USB devices containing school data must not be used on personal laptops, desktop computers or unauthorised devices.

Responding to Misuse of ICT

Pupils

Incidents involving pupils misusing school IT systems or the internet will be dealt with in accordance with the school's Behaviour Policy.

Responses will be proportionate to the nature and seriousness of the incident.

Staff

Where an employee misuses school ICT systems, the internet or personal devices covered by school policy, the matter may be dealt with under the School Code of Conduct.

The response will depend on:

- The circumstances of the incident
- The seriousness of the misconduct
- Any safeguarding or legal concerns.

The school will refer illegal activity to the police.

Training

Staff Training

All staff receive safeguarding and child protection training, which includes online safety training, during their induction. All staff receive annual safeguarding refresher training and regular updates throughout the year.

Staff Will Be Trained To Understand:

- The role technology plays in safeguarding and wellbeing concerns
- Risks of online abuse and exploitation
- How safeguarding concerns may present differently in pupils with SEND
- The importance of providing additional pastoral and communication support for pupils with SEND.

Online Risks Covered in Training

Staff will be aware that children may experience:

- Abusive, harassing or misogynistic online messages
- Non-consensual sharing of nude and semi-nude images
- Exposure to abusive images or pornography
- Online elements of physical abuse, sexual violence and initiation or hazing behaviours.

Training Outcomes

Training supports staff to:

- Identify signs of online abuse
- Help pupils recognise online risks
- Enable pupils to make safe and informed choices online
- Promote long-term online safety and wellbeing.

DSL and DDSL Training

The DSL and Deputy DSL will:

- Complete DSL training, including online safety, at least every two years
- Update their knowledge and skills annually.

Governors and Volunteers

- Governors receive online safety training as part of safeguarding training
- Volunteers receive appropriate training and updates where relevant

Further details can be found in the Safeguarding and Child Protection Policy.

Technical safety

At Cherry Orchard, all staff and pupils have access to the Internet. We use Smoothwall to filter and protect children from inappropriate websites and images. If any inappropriate data is viewed, staff are

to report it to the network manager in the first instance or subsequently the DHT, who will then contact the provider.

Computer usage of staff and pupils is also monitored by the school using Securus software. This software helps protect students by monitoring, capturing and alerting (in real time for serious incidents) the Headteacher, Deputy Headteacher and Lead DSL to potentially harmful content or behaviour, thus allowing for intervention to stop inappropriate and potentially harmful computer use, whether it involves just looking or active participation. Any items of concern are logged on our behaviour monitoring system, CPOMs, and dealt with by the Headteacher, Deputy or Lead DSL. All users are reminded that any information that they view on a school machine can be logged on Securus.

The school uses Sophos anti-virus protection on all machines. The technical support team are responsible for removing any viruses that do infect computers.

Social networking

Personal use

Staff and pupils are not permitted to use social media for personal use during lesson time.

Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.

Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behaviour Policy.

Use on behalf of the school

The school's official social media channels are only used for official educational or engagement purposes.

Staff members must be authorised by SLT to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

The school website

The headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

Personal information relating to staff and pupils is not published on the website.

Images and videos are only posted on the website if permissions are gained.

Use of personal devices

Any personal electronic device that is brought into school is the responsibility of the user.

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency and agreed by SLT.

Staff members are not permitted to use their personal devices to take photos or videos of pupils.

If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action will be taken.

The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use.

Mobile phones and smart watches brought to school by pupils are placed in the safe as per the mobile per the mobile phone and wearable technology policy.

Pupils' devices can be searched, screened and confiscated in accordance with the behaviour policy.

If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices.

Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

Use of Digital Video and Images

The developments of digital images and videos have significant benefits within the curriculum and enhance learning. Image and videos can either be taken by staff and pupils for educational purposes or downloaded from the internet to support learning in the classroom. However, staff and pupils need to be aware of the risks associated with sharing images, especially via the internet. Staff and pupils need to be aware that once an image/video is posted on the internet, it will remain there forever. This could cause harm or embarrassment in the future.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational purposes, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken that when capturing images/ videos that all pupils concerned are appropriately dressed and not participating in activities that could bring either the pupils or the school into disrepute.
- Pupils' full names will not be used anywhere on the website or in blogs and particularly not associated with photographs on there.

- Parents are asked when their child begins school whether they wish for their child's pictures to be published on the school website, newsletter or social media. A record of this is sent to the class teacher (stored in the class register).
- Cherry Orchard Primary School will always comply with GDPR in regards to digital images and videos.

Reporting Online Safety issues

All children will be made aware of the importance of reporting any incident to either an adult at school that they can trust regarding any incidents that may occur outside of school.

Online safety incidents will be recorded on CPOMs.





Staff Acceptable Use Policy

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head Teacher and Governing Body.
- I will not allow unauthorised individuals to access email / Internet / intranet /network, or other school / Local Authority systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will use Microsoft Copilot AI as a tool to support high-quality teaching supported by CPD and recommendations in the EEF guidance report, 'Using digital technology to improve learning'.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I understand that failure to comply with this agreement could lead to disciplinary actions.

User Signature

I agree to abide by all the points above. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety policies.

Signature: _____ Date: _____

Full Name _____ (printed)