Orchard Lea Federation

Online Safety Policy

Date agreed: November 2025

Date for renewal: November 2026

Aims

Our federation aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology, which can include but are not limited to:
  - Internet browsers and search engines
  - Email
  - Instant messaging (often using simple web cams) e.g. WhatsApp, iMessage)
  - Web based voice and video calling (e.g. Skype, Facetime, Zoom)
  - Online chat rooms
  - Online discussion forums
  - Social networking sites (e.g. Facebook, Instagram, Snapchat)
  - Blogs and Micro-blogs (e.g. X, Threads)
  - Podcasting (radio / audio broadcasts, downloaded/watched or listened to)
  - Video broadcasting sites and livestreaming (e.g. You Tube, Tik Tok, Twitch)
  - Homework learning platforms (TTRS, MyMaths)
  - Google apps (e.g. classroom, docs, slides)
  - Music and video downloading (e.g. Apple Music, Spotify)
  - Mobile phones with camera and video functionality
  - Smart phones with e-mail, messaging and internet access 2 November 23
  - Artificial intelligence (Amazon Alexa, Google assistant, Siri, Chat GPT)
  - Virtual reality
  - Online Video Gaming

1. The 4 key categories of risk

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

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

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education
- Searching, screening and confiscation
- It also refers to the DfE's guidance on protecting children from radicalisation.
- It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.
- The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Governing body

- The Governing body has overall responsibility for monitoring this policy and holding the Executive 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 as provided by the designated safeguarding lead (DSL).

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 IT systems and the internet through reviewing the policies each year.
- Ensure that online safety is a running and interrelated theme while devising and implementing the whole federation 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 Executive Headteacher

The Executive Headteacher is responsible for:

- Ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- Working with the Heads of School and IT provider to ensure that monitoring and filtering systems are keeping pupils safe and effective.

3.3 The Designated Safeguarding Lead

- Details of the school's designated safeguarding lead (DSL) deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.
- The DSL takes lead responsibility for online safety in school, in particular:
- Supporting the Executive Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Executive Headteacher, and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy. (Ensure Computing Leads are tagged in so they can monitor)
- 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 2 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 Executive Headteacher and/or Governing body.

3.4 The IT Providers

The IT provider is responsible for:

- Working with Leaders to put in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT 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 IT systems on a monthly basis.
- Working to block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

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 IT systems and the internet and ensuring that pupils follow the school's terms on acceptable use (appendix 2).
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here.'

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Executive Headteacher of any concerns or queries regarding this policy.
- 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 International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

- Visitors and members of the community who use the school's IT 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 (see acceptable use policy).

4. Educating pupils about online safety

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

  All schools have to teach:

- Relationships education and health education in primary schools.

  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.
- 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.
- Make children aware of misinformation, disinformation and conspiracy content as potential safeguarding harms. (maybe through ecadets)

- Educating children the risks about generative AI and emerging digital technologies.
- 5. Educating parents about online safety
- The schools will raise parents' awareness of internet safety in newsletters or other communications home, and in information via our website. This policy will also be shared with parents via the website.

  The school will let parents know through newsletters:
- What systems the school uses to filter and monitor online use.
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of School and/or the DSL.
- Concerns or queries about this policy can be raised with any member of staff.

6. Cyber-bullying

6.1 Definition

- Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the federation behaviour policy and anti-bullying policy).

6.2 Preventing and addressing cyber-bullying

- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.
- 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.
- The school also sends information/leaflets on cyber-bullying to parents 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 Curriculum leader for computing will also analyse any incidences in order to adapt the curriculum provision and review training.
- The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

If staff suspect that there may be something on devices that:

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

Staff will contact the parents and ask them to view the content.

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

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

  UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.
- 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 (see also the acceptable use policy)

- All staff, will adhere to the acceptable use of the school's IT systems and the internet policy. 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.

8. Staff using work devices outside school

- All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:
- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date by always installing the latest updates.

- Staff members must not use the device in any way which would violate the school's terms of acceptable use.
- Work devices must be used solely for work activities.
- If staff have any concerns over the security of their device, they must seek advice from the school's IT provider.

9. How the school will respond to issues of misuse

- Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies on behaviour and IT acceptable use policies. 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 IT 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 code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
- The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10. Mobile Phones and Smart watches

- Pupils in Years 5 and 6 only are permitted to bring phones to school. All pupils must place their phones into a class box which will be kept in the office until the end of the school day.
- Pupils are not permitted to wear smart watches in either school.

11. Filtering and Monitoring

The federation will ensure that there are effective monitoring and filtering systems in place in line with the expectations of KCSIE. This will be through;

- Weekly reports to the Heads of School and Executive Headteacher from the IT providers. Checking the parameters of what is included in the filtering systems set up by the IT providers.
- Half termly checks on a selection of devices in school.
- Ensuring that all staff and pupils know how to report a concern and Leaders monitoring/actioning concerns raised.
- Following up any concerns raised in any of the reports/actions listed above.

12. Training

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

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

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- We recognise that children can abuse other children online through:
    - Abusive, harassing, and misogynistic messages.
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
    - Sharing of abusive images and pornography, to those who don't want to receive such content.
- All concerns regarding child on child abuse will be dealt with in accordance with our child protection policy.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

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

13. Monitoring arrangements

- The DSL logs behaviour and safeguarding issues related to online safety on the CPOMS system.
- This policy will be reviewed every year by the Executive Headteacher and IT Leaders. At every review, the policy will be shared with the Governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14. Links with other policies

This online safety policy is linked to key polices such as our:

- Child protection policy
- Safeguarding policy
- Behaviour policy
- Anti- Bullying policy

- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- IT acceptable use policy
- Social Media Policy
- Whistleblowing Policy

Appendix 1: Internet use in school- possible teaching and learning activities

Activities	Key Online Safety issues	Relevant websites
Using search engines to access information from a range of websites.	Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Some search engines children may use: Bing Google DuckDuckgo Ecosia
Publishing pupils' work on school website.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	School website
Publishing images including photographs of pupils	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	School website

Appendix 2: 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)**

ONLINE SAFETY TRAINING NEEDS AUDIT	
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
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?	