The Oakridge Schools Federation

Online Safety Policy

Approved by:	Full Governing Body
Review frequency:	Every 2 years
Date last approved:	Autumn 2025
Next review date due:	Autumn 2027

Introduction

Online safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits as well as the risks of using new technology. This policy is designed to provide safeguards and awareness for users to enable them to control their online experiences.

The school's online safety policy will operate in conjunction with other policies including those for:

- Anti-Bullying
- Behaviour
- Safeguarding
- PSHE & Health and Wellbeing

Online safety depends on effective practice at a number of different levels:

- Responsible IT use by all staff, governors and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of content filtering.

Internet (World Wide Web)

- If staff, governors or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Computing subject leader or Executive Headteacher or School Business Manager, who will contact the IT Systems Management Company, Harrap ICT or Local Authority, where appropriate, to block said site
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The list of blocked websites will be reviewed annually by senior leaders and the Governing Body.

Social Media

As a school, we recognise that social media and networking are playing an increasing role within everyday life and that many staff and governors use tools such as Facebook, Instagram, Twitter and Snapchat, using these for both personal and professional use. We will ensure that all staff, governors, and children are kept fully aware of the risks and issues that may arise, as well as the ways to minimise these risks.

As a school, we block access to social networking sites on children's devices and through wireless internet access.

Social media networks (Facebook, X and Instagram) can be accessed on staff devices using staff logins. This is to allow staff to update the school's social media accounts.

Staff and governors should:

- Ensure that their profile and posts are kept private to friends where possible. This also includes personal information, such as phone numbers and email addresses.
- Not accept current or former pupils as 'friends' on social media sites such as Facebook. This is to ensure that there is no possible misinterpretation. We understand that some staff members live and have friends within the local community, and we ask that these members of staff take extra care when posting online.
- Ensure that their communication always maintains their professionalism.
- Be aware that electronic texts can be misconstrued, so should endeavour to minimise the possibility of this happening.
- Not use these media to discuss confidential information or to discuss specific children.
- Check with the Computing subject leader or IT Technician if they need advice on monitoring their online persona and checking their security settings.

Pupils should not be signed up for most social networking sites due to the age limit of 13 and above. However, we recognise that some are signed up with, or without, parental knowledge. As a school, we will monitor the use of social networking and ensure it's part of our Computing curriculum. We will ensure that parents are made aware of how to minimise the risk if their children are using these sites. As a school, we do reserve the right to contact sites such as Facebook and ask them to remove our children's accounts should any issues, such as cyberbullying, arise.

Information system security

- School ICT systems security will be reviewed regularly
- Virus protection is updated and managed regularly
- Security strategies will be discussed with IT Systems Management Company, Harrap ICT or the Local Authority, where appropriate.

Filtering

The school will work in partnership with the Local Authority and the Internet Service Provider to

ensure filtering systems are as effective as possible. This will be reviewed regularly by the governing body and senior leaders.

Following guidance from KCSIE (2025), the school monitors users' web searches. Should a user's search history be flagged as inappropriate, the Computing Subject Lead and School Business Manager will be notified. Depending on the nature of the search, the Computing Lead or School Business Manager will then investigate and speak to the appropriate children, parent or member of staff. Incidents where children have accessed inappropriate content or terms will be recorded on CPOMs.

Managing Emerging Technologies/Future developments
Emerging technologies will be examined for educational benefits, and a risk assessment will be carried out before their use in schools is permitted. This policy will be amended as required.

Cloud Server
Oakridge Schools Federation utilises a platform that allows users to access a cloud server remotely (off-site). This is managed in conjunction with our network administrator/manager, Harrap ICT. All staff members who have access to the cloud server outside of school have signed the appropriate acceptable use policy. When accessing the cloud server off-site, staff must ensure that any personal data or information is stored securely.

Use of Memory Sticks (and other portable storage)
In line with GDPR (General Data Protection Regulation), all staff are no longer permitted to use memory sticks or other portable storage devices. Relevant staff have access to the school's cloud server and have signed the acceptable usage policy for using off-site.

Published Content and the School Website

- The contact details on the website should include the school's address, admin office emails, and telephone numbers.
- Staff, governors or pupil's personal information will not be published.
- The Executive Headteacher, Deputy Headteacher, School Business Manager, and Computing subject leader will take overall editorial responsibility and ensure that the content published is accurate and appropriate to the public.

Publishing Digital and Video and Images
We follow these rules to maintain safety on our school website:

- For a photograph of a child to be published and appear on our school website, consent must be obtained from the parent or guardian of the child. This consent is obtained on admission to the school and is reviewed regularly. Any parent or guardian may withdraw their consent at any time.
- If we do not have permission to use the image of a particular child, we will make them unrecognisable to ensure they are not left out of the situation necessarily.
- We will not use the personal details or full names of any child or adult in a photographic image or video, on our website, in our school prospectus or in any of our other printed

publications without good reason. For example, we may include the full name of a pupil in a newsletter to parents if the pupil has won an award.

- If we name a pupil in the text, we will not use a photograph of that child to accompany the article without good reason. (See above)
- We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.
- Personal information about children or staff is not shared on our website. Contact e-mails are only provided for the School Admin Office.
- All information on the school website is published by teaching staff and administrative staff; however, only certain staff members are labelled as 'Admin' for the website, who have editing access to the entire site. This avoids content on the website inadvertently contravening these rules.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school, IT Systems Management Company, Harrap ICT nor Hampshire County Council can accept liability for the material accessed, or any consequences of Internet access.
- The school should review IT use to establish if the online safety policy is sufficient and that the implementation of the online safety policy is appropriate. This policy is reviewed annually, with termly health checks.

Handling Online Safety Complaints

- Complaints or Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Executive Headteacher.
- Complaints relating to Safeguarding must be dealt with in accordance with the Federation Safeguarding Policy.
- Pupils and parents will be informed of the Federation Complaints Procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Online safety incidents will be responded to in accordance with the flowchart in Appendix A.

Communication of Policy

Pupils

- Pupils will be informed that Internet use will be monitored.
- Sign 'Acceptable Use' agreement.

Staff and Governors

- All staff and governors will be given the School's Online Safety Policy and its importance explained.

- Staff and governors should be aware that Internet traffic is monitored and traced to the individual users. Discretion and professional conduct is essential.
- Sign 'Acceptable Use' agreement.

Parents

- Parent's attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and on the school websites.

Appendices

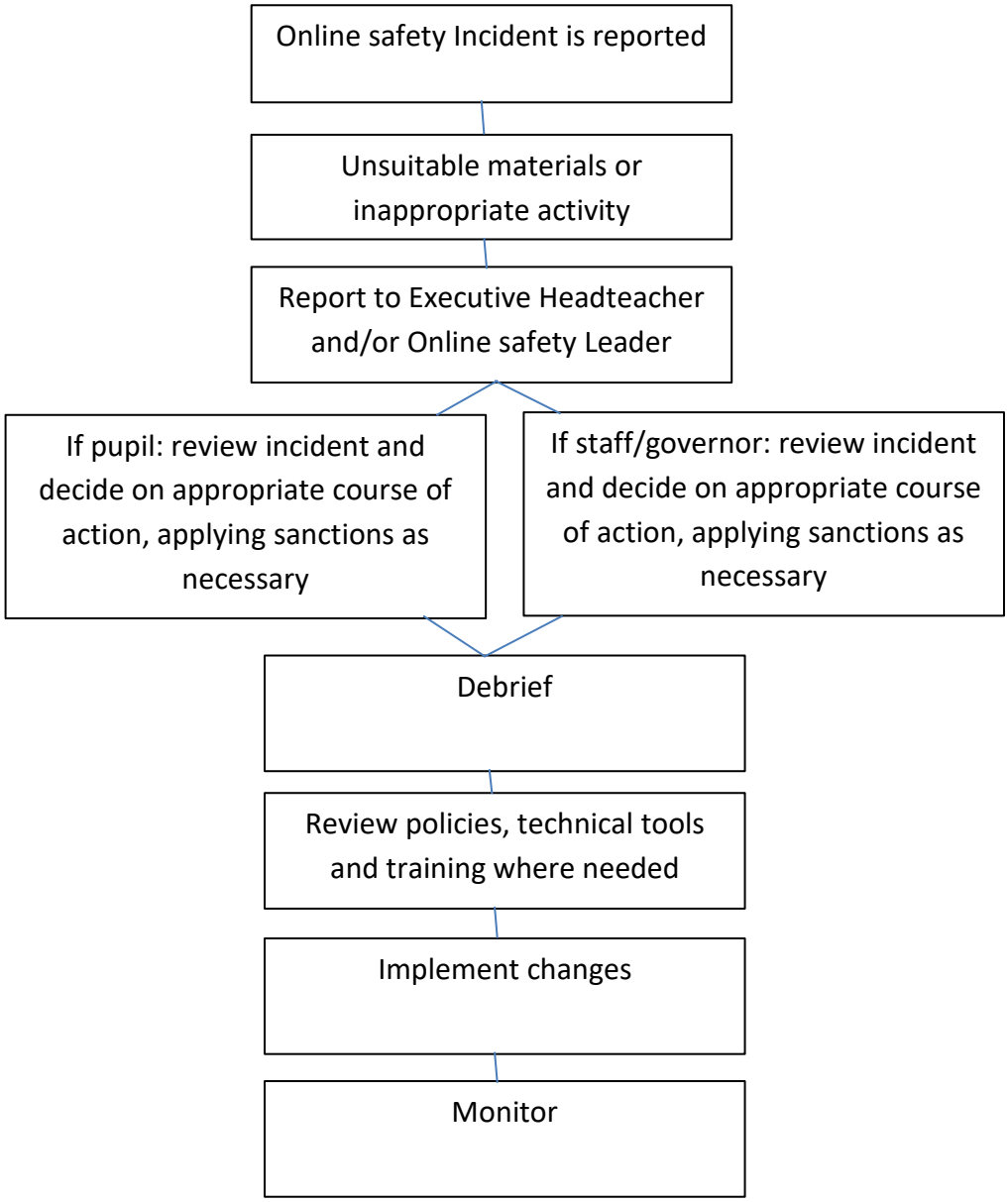
Responding to Online safety Incidents – Appendix A

Pupil Acceptable Use Policy – Appendix C

Staff and Governors Acceptable Use Policy – Appendix D

Appendix A

This flowchart is used for responding Online safety incidents at The Oakridge Schools Federation



Key Stage 2 Internet Safety Rules

Think then Click!

We ask permission before using the Internet.

We tell an adult if we see anything we are uncomfortable with.

We send e-mails and messages that are polite and friendly.

We never give out personal information or passwords but we can share them with our parents

We never arrange to meet anyone we don't know

We do not open e-mails sent by anyone that we do not know.

We do not use Internet chatrooms.

Appendix C

Acceptable Use Policy for Foundation Stage and KS1 Children

I want to feel safe all the time.

I will:

- Keep my password a secret
- Only open pages that my teacher has said are OK
- Only work with people I know in real life
- Tell my teacher if anything makes me feel scared or uncomfortable
- Not share my personal details with anybody

I know that anything I do on the computer may be seen by someone else.

Appendix D

Staff and Governors Acceptable Use of IT

Staff Information Systems Code of Conduct

Purpose: to ensure that staff and governors are fully aware of their professional responsibilities when using information systems. Staff and governors should consult the school's online safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes without specific permission from the Executive Headteacher.
- I understand that the school may monitor my use of information systems and Internet usage to ensure policy compliance
- I will respect system security and not disclose any passwords or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without prior permission.
- I will ensure that personal data is kept secure and used appropriately, whether in school, taken off school premises, or accessed remotely.
- If I have use of a school iPad, I accept full responsibility for the device and will report any faults immediately to the appropriate person. I will also ensure that an appropriate password is installed in line with the Confidentiality policy.
- I will respect copyright and intellectual property rights.
- I will report any incidents or concerns regarding children's safety to the school Online Safety Leader/Computing Subject Lead or the Designated Safeguarding Leader (DSL)/Deputy Designated Safeguarding Leaders (DDSL)
- I will ensure that any electronic communication with pupils are compatible with my professional role.
- I will promote online safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Signed …… **Date…….**