Online Safety Policy

Rationale

Online Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. This policy is written in line with 'Keeping Children Safe in Education' 2025 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents.

The school's Online Safety Policy operates in conjunction with other policies including those for Child Protection, Behaviour, Anti-Bullying, Mobile Phone, Children's Mobile Phone, and Data Protection.

End to End Online Safety

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

- Responsible ICT use by all staff and pupils, encouraged by education and made explicit through published policies.
- Sound implementation of the Online Safety Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from RM Broadband including the effective management of filtering.
- National Education Network standards and specifications.

Writing and reviewing the Online Safety policy

- The school's Online Safety coordinator and Designated Child Protection Officer is Steve Smith (headteacher). He liaises with the Pupil Support Team around issues to do with Online Safety as their roles overlap. There is a designated Online Safety governor (Jason Toft).
- Our Online Safety Policy has been written by the school, building on the Stoke-on-Trent Internet Safety Policy and government guidance. It has been agreed by senior management and approved by governors.
- The Online Safety Policy and its implementation is reviewed annually.

Online Safety Audit

The Online Safety coordinator completes an annual Online Safety Audit with the head teacher, the lead learning mentor, SENCO and school business manager. Other members of the team may also contribute where necessary. The audit can be found at the end of this document (Appendix 1)

Teaching and Learning

Why are new technologies and Internet use important?

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet to enhance learning

- The school Internet access is designed for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and are given clear objectives for Internet use.
- Online access is planned to enrich and extend learning activities. Access levels are reviewed by the online safety coordinator upon requests from staff to reflect the curriculum requirements and age of pupils.
- Staff guide pupils in on-line activities that support the learning outcomes planned for the pupils' age and maturity.
- Pupils are educated in the effective use of the Internet in research, including the skills of effective knowledge location, retrieval and evaluation.
- Pupils are taught about age appropriate apps and online safety when using tablets or mobile devices.
- In 2025, the school introduced 1:1 iPads for pupils in Years 2 – 6. Regular work is done with pupils and staff to ensure that pupils use these in a safe manner.

Pupils are taught how to evaluate Internet content

- The school ensures that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils are taught how to stay Internet safe

- At Oakhill, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety).

- Curriculum planning includes age appropriate opportunities to discuss, role play and learn about the benefits and risks offered by technologies, such as e-mail, mobile phones, apps and social networking sites.

- The schools Online Safety curriculum is mapped throughout the Computing curriculum and PSHE Jigsaw curriculum to ensure that it is re-visited regularly. There are also stand alone Online Safety units in each year group.

- Each year group does a minimum of 6 dedicated online safety sessions per year. This is addition to the online safety work covered in computing sessions, in the PSHE Jigsaw scheme and on National Online Safety Day.

- As advised in RSHE guidance, we assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self evaluations, to capture progress." To support us with this we use LGFL's Safeskills Online Safety Quiz twice per year to assess where our pupils biggest learning needs are.

AI

AI in schools can improve education by personalising learning and making education more accessible. Staff use AI to further improve teaching and learning through:

- Lesson planning and curriculum enhancement
- Adaptive learning for differentiated instruction.
- SEND support, ensuring accessibility and inclusion.
- Pupil assessments (ensuring integrity and compliance with assessment policies).

AI is not used in a way that compromises ethics, student safety, data privacy, fairness, or academic integrity.

See AI policy for further information.

Managing Internet Access

Information system security Virus protection is updated regularly on all networked computers by the school's ICT support provider (RM).

- School ICT systems capacity and security are reviewed regularly by the school's ICT support provider (RM).
- Security strategies are discussed by the Online Safety coordinator and the school's named ICT support technician (provided by RM) regularly and at senior leadership meetings as appropriate.
- Only links from trusted sources are published on the school website.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils are taught that the same rules apply when using the school email system at home and that this can still be monitored. Pupils are also taught about the benefits/drawbacks of different email systems.

The School Website

- The school's website is hosted by Primary Site which is now part of Juniper Education.
- Parents, staff and pupils have designated access to appropriate pages.
- Images of pupils are selected carefully, ensuring that the necessary consent has been sought from parents/carers BEFORE publication.
- Only images that have no copyright restrictions are used on the website.
- Written permission from parents or carers is obtained before images of pupils are electronically published to the web.

Social networking and personal publishing

- The school has a separate social networking policy and acceptable use agreement, which are signed by every member of staff upon their induction.
- The school block/filter access to social networking sites, except those specifically purposed to support educationally approved practice.
- Staff and pupils are advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents are advised that the use of social network spaces, outside school based controlled systems, is inappropriate for primary aged pupils
- Members of staff do not contact users who are ex pupils and under the age of 16. Staff are advised not to contact any former pupils, regardless of age, on social media.
- Staff are advised to maintain the highest levels of professionalism when posting on social networking sites. Where this does not happen, staff may be subject to disciplinary procedures as per the school's disciplinary policy.
- Photographs of children are not used without parents/carers permission especially in the press and on the internet
- Online safety alerts are sent to parents/carers as and when needed. For example, when any new guidance is available or when there is a particular issue either in school, locally or nationally.

Misuse of school technology (devices, systems, networks or platforms)

- Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).
- These are defined in our Acceptable Use Policy as well as in this document.
- Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct.
- It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place in future periods of absence/ closure/quarantine etc.
- Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.
- The new responsibilities for filtering and monitoring, led by the DSL and DDSL's and following the new DfE standards, may mean that more such incidents will be discovered in the coming year but the school will remind pupils and staff of this increased scrutiny at the start of the year.

<u>Managing filtering and monitoring</u>

- Web filtering is provided by RM Safety Net for all school devices. Our Internet provider is RM Broadband.
- Changes can be made by Steve Smith, Helen Dodd, Will Weaver (the school's RM ICT technician). Support and advice is sought from RM when changes need to be made to ensure best practise.
- Overall responsibility is held by the DSL (Steve Smith) and DDSL (Helen Dodd, Jo Somogy, Katie Hawthorne)
- Technical support and advice, setup and configuration are from RM (the school's IT support provider)
- regular checks are made half termly by Steve Smith to ensure filtering is still active and functioning everywhere. These are evidenced in the safeguarding file.
- The school work with our Internet provider (RM Broadband) to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, the URL must be reported to the school Online Safety Coordinator, any member of SLT or the headteacher

- Monitoring software (Smoothwall) is used in school and is monitored weekly by the Deputy Headteacher (Helen Dodd), with the Headteacher then monitoring the Deputy Headteacher. This is to identify inappropriate use or misuse, or to identify evidence of grooming or self-injurious behaviour which could indicate that actions should be taken under the safeguarding policy. This is for both staff and pupils.

Managing remote teaching/video calling (including Teams and Zoom)

Users

- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing is supervised appropriately for the pupils' age.
- Unique log on and password details for the educational videoconferencing services are only issued to members of staff and kept secure.

Content

- Recorded material is stored securely.
- If third-party materials are included, recordings are checked to ensure that they are acceptable to avoid infringing the third party intellectual property rights.
- Dialogue is established with other conference participants before taking part in a videoconference. If it is a non school site it is checked that they are delivering material that is appropriate for the class.

Mobile Phones

- Pupils are not allowed to use mobile phones during lessons or formal school time. For further information see the attached 'Pupils Use of Mobile Phones' policy.
- The school's Parentmail/Dojo services are used in all circumstances where text contact with parents is necessary.
- Staff do not use personal mobile phones to contact parents except in an emergency and where no other options are available (for example, on a trip)

Protecting personal data

- Personal data is recorded, processed, transferred and made available according to General Data Protection Regulations (GDPR) 2018.

Artificial intelligence

(AI) Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT. Oakhill Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to harm others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. We will treat any use of AI in this way in line with our behaviour policy and/or staff code of conduct. Staff should be aware of the risks of using AI tools whilst they are still being developed and should seek advice for the Senior Leadership Team where required.

Policy Decisions

Authorising Online access

- The school maintains a current record of all staff and pupils who are granted access to the school's electronic communications, which includes Online access. The record is kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- All staff must read and sign the 'Code of Conduct', 'Social Networking Policy' and 'Acceptable Use Agreement' before using any school ICT resource.
- At Foundation Stage, online access is by adult demonstration or by directly supervised access to specific, approved on-line materials.
- Parents are given the option to withdraw their pupils from using the Internet at school should they wish

Assessing risks

- The school take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Orchard Community Trust Council can accept liability for the material accessed, or any consequences of online access.
- The school audit ICT provision to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks are reviewed regularly.

Handling online Safety complaints

- Complaints of Online misuse are dealt with by a senior member of staff (usually Steve Smith)and are always recorded on the school's CPOMS system for safeguarding.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents are informed of the complaints procedure.
- Parents and pupils then work in partnership with staff to resolve issues.
- Sanctions within the school behaviour policy include (but not be limited to):
    - One to one or group work with the learning mentor team or a member of the Online Safety team;
    - informing parents or carers;
    - removal or restriction of Internet or computer access for a period.
    - Where applicable, other agencies (including the police and social care) may be contacted.

Cyberbullying

Understanding and addressing the issues

While cyberbullying is very rare at Oakhill Primary School, the age of pupils making proficient use of technology is ever decreasing. Therefore, the opportunities for pupils to bully or be bullied via technology, such as text messaging and social networking sites are becoming more frequent.

As such, teaching pupils about appropriate behaviours when using technology provides a vital grounding for future use. Whilst not wanting to provoke unrecognised opportunities in pupils, consideration must be given to suitable teaching and procedures to address any issues of cyberbullying.

As felt appropriate for the age and use of technology by the pupils:

- The school's anti-bullying policy and school behaviour policy addresses cyberbullying. Cyberbullying is also addressed in Computing, PHSE and other relevant lessons and is brought to life through activities. .

- Pupils, parents, staff and governors are made aware of the consequences of cyberbullying. Young people and their parents are made aware of pupils' rights and responsibilities in their use of new technologies, and what the sanctions are for misuse.
- Parents are provided with an opportunity to find out more about cyberbullying through: annual parents sessions, Online safety message alerts and via the school website.
- Pupils, parents, staff and governors are made aware, at the appropriate level, of the possibility of others using the Internet for the purposes of child sexual exploitation. This is in the form of training, parent awareness meetings and pupil lessons.

How are risks assessed?

The school proactively engage with all pupils in preventing cyberbullying by:

- understanding and talking about cyberbullying, e.g. inappropriate use of e-mail, text messages, social media etc.
- planning effective, progressive Online Safety lessons for each year group
- keeping existing policies and practices up-to-date with new technologies;
- ensuring easy and comfortable procedures for reporting;
- promoting the positive use of technology;
- evaluating the impact of prevention activities.

- Records of any incidents of cyberbullying are reported to the Headteacher and are used to help to monitor the effectiveness of the school's prevention activities. A log of these are kept on the school's CPOMS system for safeguarding.
- Methods to identify, assess and minimise risks are reviewed regularly.

How are cyberbullying reports/issues handled?

- Complaints of cyberbullying are dealt with by a senior member of staff and a log is kept on the school's CPOMS system for safeguarding.
- Any complaint about staff misuse must be referred to the headteacher.
- Evidence of offending messages, pictures or online conversations are kept and saved to the school's CPOMS system, where possible, in order to demonstrate to others what is happening. It can then be used by the school, internet service provider, mobile phone company, or the police, to investigate the cyberbullying.
- Pupils and parents are informed of the complaints procedure.
- Parents and pupils work in partnership with staff to resolve issues.
- Sanctions within the school behaviour policy include (but are not limited to):
  - One to one or group work with the learning mentor team or a member of the Online Safety team;
  - informing parents or carers;
  - removal or restriction of Internet or computer access for a period.
  - Where applicable, other agencies (including the police and social care) may be contacted.

<u>Introducing the Online Safety Policy to pupils</u>

- Child friendly Online safety rules are displayed in all networked rooms and discussed with pupils at the start of each computing session and as the need arises.
- Pupils are informed that network and Internet use is monitored.
- Online Safety staff updates take place at least every half term to keep staff up to date with the latest developments in this area which they can then pass onto to pupils.

- Reminders of responsible and safe use always precede Internet access.

Staff and the Online Safety policy

- All staff are given the school's Online Safety Policy and its application and importance explained.
- All staff are informed that all computer and Internet use is monitored. Discretion and professional conduct is essential.
- Staff training/briefings in safe and responsible behaviour online and on the school's Online Safety Policy are provided at least 6 times per year, one of these is an extended session to do this in more depth.
- Staff that manage filtering systems or monitor ICT use are supervised by the senior leadership team and have clear procedures for reporting issues.

Enlisting parents' support

- Parents are reminded about the school's Online Safety Policy in monthly newsletters, on the school website, on the school Facebook page and through parents' sessions.
- Parents receive a monthly online safety newsletter which alerts parents to the most current online safety risks.
- Online safety awareness sessions are held for parents at least twice a year. These sessions also focus on the most current online safety risks to ensure that they are of most benefit.
- The school also uses any assemblies where parents come in to school to pass on important online safety reminders.
- Online issues are handled sensitively, and parents are advised accordingly.
- A partnership approach with parents is encouraged. This includes sessions with parents either in groups or on a one to one basis as required.

REVIEW & AMEND AS NECESSARY ANNUALLY – SEPTEMBER 2027 (MOST RECENT REVISION JUNE 2025)

Appendix 1: Online Safety audit

Has the school an Online Safety Policy that complies with national guidance?	**Yes**
Date if latest update (annually)	**August 2025**
The school Online Safety Policy was agreed by governors on	**September 2025 (J.Toft)**
The policy is available for staff	**Teams and website**
The policy is available for parents/carers	**Website and school office**
Member of the senior leadership team responsible for Online Safety	**Steve Smith**
Member of the governing body responsible for Online Safety	**Jason Toft**
Designated person for Child Protection	**Steve Smith**
Data Protection Officer	**Danielle Cartner**
Online Safety coordinator	**Steve Smith**
Online Safety team	**Steve Smith, Alice Warner, Katie Hawthorne, Helen Dodd**
Has Online Safety training been provided for all staff?	**Yes – completed each half term**
Has Online Safety guidance been provided for all pupils?	**Yes – in lessons and displayed**
Are Online Safety guidance materials available for parents?	**Yes – website, school office**
Is there a clear procedure for a response to an incident of concern?	**Yes**
Have Online Safety materials from CEOP been obtained and used?	**Yes**
Do all staff sign an Acceptable Use Policy and Social Network policy on appointment?	**Yes**
Are pupils aware of the school Online Safety rules?	**Yes – regular reminders in lessons**
Have all parents/carers signed an Online Safety home/school agreement form?	**Yes**
Are Online safety rules displayed in all rooms accessed by pupils?	**Yes**
Has an ICT security audit been initiated by SLT?	**Yes**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Yes**
Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements?	**Yes – RM Broadband with RM Safety Net**
Has filtering on Internet-based devices been appropriately applied?	**Yes**