Online Safety Policy

Approved: January 2025

Contents:

Rationale

Keeping Children Safe in Education 2024 states: *"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate"*

In a rapidly changing world, that is increasingly transformed by technology, Oak Learning Trust schools endeavour to equip children with the skills needed to use technology to become independent and creative learners that do so in a confident but safe manner. Technology affects how children live and the activities they choose to partake in and, in many areas, technology continues to transform the ways children learn and how schools teach. Just as there are many benefits to these technologies (including the Internet), there are also many risks too, and so the online safety policy encourages appropriate use and safe conduct.

Our trust policy aims to promote the use of the Internet safely, responsibly, and positively to all members of the school community (including staff, pupils, volunteers, parents/careers, visitors and community users), who have access to and are users of school ICT systems, both in and out of school. This policy explains how the trust strives to keep children safe within school, when using technology, but also how we educate children of the potential risks when using technology in other situations (e.g. at home). We achieve this through delivering the computing curriculum that has been adapted specifically to the requirements, age and needs at our school. This policy is interlinked with various safeguarding policies and other policies including personal, social and health education (PSHE). The ultimate aim of our policy is to safeguard children online.

The purpose of our online safety policy is to:

- Raise awareness to the potential benefits and risks of technology, with all members of the school community.
- Identify clear procedures, known by members of the school community, for responding to online safety concerns.
- Protect and safeguard all members of the school community online.
- To enable all staff (including volunteers/students), to promote and model positive behavior online and work safely and responsibly by being aware of the need to manage their own practice and standards when using technology.
- To have clearly identified key principles with regards to safe and responsible use of technology, expected by all members of the community, to ensure our school is a safe and secure environment.

The online policy will be monitored annually by the trust Computing Lead and changes recommended to the board. If serious online incidents occur, the school will inform and take advice from social services and the policy if necessary. Each school will deal with such incidents under the provisions within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online incidents covered by this policy, which may take place outside of the school, but are linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Policy and Leadership

All those working within the Oak Learning Trust are committed to safeguarding children in our care and online safety is an essential element of this. Therefore, this policy reflects on our thorough approach to safeguarding.

Roles and Responsibilities

All schools within Oak Learning Trust are a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school and trust. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Trust board

- Ensure all schools and trust central staff follow all current online advice to keep children and staff safe.
- Approve the online policy and monitor and review its effectiveness.
- Work with Director of Learning and Performance to ensure a compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring).

Governors

- Ensure the school follows all current online advice to keep children and staff safe
- Ensure the implementation of the online policy and monitor and review its effectiveness
- Have regular reviews with computing lead and Designated Safeguarding Lead (DSL)
- Monitor the online safety incident log regularly
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards, this may be the safeguarding governor.
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DSL and headteacher/Head of School to ensure a compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring

Executive Headteacher/Headteacher/Head of School

- To take overall responsibility for online provision
- To ensure all staff have read and understood this policy.
- To take overall responsibility for data and data security
- To ensure the school uses an approved, filtered Internet Service through One IT services
- To be responsible for ensuring that staff receive suitable training to carry out their roles and to train other colleagues to ensure they are aware of online dangers
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance
- Ensure ALL staff undergo safeguarding training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- To receive regular monitoring reports
- Liaise with the designated safeguarding lead on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DSL and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised.
- Ensure the school website meets statutory requirements

Designated Safeguarding Lead, deputy/deputies

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents (including online safety and understanding the filtering and monitoring systems and processes in place)
- Promotes an awareness and commitment to online safeguarding throughout the school community
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated. This must include filtering and monitoring and help them to understand their roles.
- Ensures that online safety education is embedded across the curriculum
- Liaises with school computing technical staff and external service providers (One IT)
- To communicate regularly with SLT and the designated Online safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs
- To ensure that all staff are aware of the procedures that need to be followed in the event of an online Safety incident
- To ensure that an online safety incident log is kept up to date
- Facilitates training and advice for all staff
- Liaises with the Local Authority and relevant agencies
- Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
  - sharing of personal data
  - access to illegal / inappropriate materials
  - inappropriate on-line contact with adults / strangers
  - potential or actual incidents of grooming
  - online bullying and use of social media

Computing Lead

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach.
- Work closely with the DSL/DDSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements.

Teachers

- To ensure the teaching of the computing curriculum and the teaching of online safety is embedded and promoted in all aspects of the curriculum
- Ensure regular online safety lessons are provided and evidenced
- To guide and supervise children when using technology within their lessons
- To comply with filtering and monitoring principles and play their part in feeding back to the DSL about overblocking, gaps in provision or pupils bypassing protections. All staff are also responsible for the physical monitoring of pupils' online devices during any session/class they are working within

All Staff

- To understand that online safety is a core part of safeguarding and, as such, is everyone's job
- To read and follow the online safety policy, signing and completing the acceptable usage policy agreement
- Record online safeguarding incidents and report in accordance with school procedures
- To model safe professional and responsible usage of technology both within and outside of school
- Ensure that all digital communication with parents is carried out using only official school systems

Technical Staff

- To develop and maintain an awareness of current online safety issues, legislation and guidance relevant to their work.
- To support the school in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the school network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the school ICT system.
- To liaise with the appropriate people and organisations on technical issues
- To restrict all administrator level accounts appropriately.
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To help maintain the filtering and monitoring systems in school and regularly meet with school leaders to ensure the system is working effectively

Pupils

- Read understand and sign the acceptable use agreement-KS1 and KS2- EYFS signed by parent.
- Understand how and why to report any abuse or misuse of digital technology
- To understand the importance of being a responsible citizen online

Parents/Carers

- To have read and understood the online safety policy
- To ensure they have read and understood the acceptable use agreement and promote it with their children
- To inform school if they have any concerns regarding their children's use of technology

Volunteers/Student Teachers/Supply Staff

- Read, understand, sign and adhere to an acceptable use policy
- Report any concerns, no matter how small, to a DSL
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications

External Groups

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers
- Will share any presentations, resources (real and online) with the school in advance so they can be vetted by the Headteacher/head of school or their delegated staff member.

Technical Staff and Security Systems

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.

- All users will be provided with a username and secure password by the school technician who will keep an up-to-date record of users and their usernames. Staff are responsible for the security of their username and password and will be required to change their password regularly (every 90 days).
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher/Head of School or other online safety lead and kept in a secure place (e.g. school safe).
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by OneIT. There is a clear process in place to deal with requests for filtering changes see filtering policy for more details.
- The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users –staff / pupils / students etc.)
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual /potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.

Security and passwords

- Passwords should be changed regularly
- The system will inform users when the password is to be changed every 90 days.
- Where passwords may have been compromised, they must be changed immediately.
- Pupils should never share their passwords or logins or allow anyone to log in as them
- Staff must not share their passwords or allow a pupil to use their login.
- Staff must always 'lock' the PC if they are going to leave it unattended.

Mobile Phones

As mobile phones often have unrestricted access to the internet and are able to send messages, picture messages and videos, there is an increased risk these could be used for bullying or the sending of inappropriate content.

To ensure the school is a safe environment and to safeguard adults and children the following apply:

- Pupils in Y5 and Y6 may bring their phones to school when it is considered essential to their safety, however, these must be switched off and handed in to be stored safely within the office or classroom until the end of the day
- Pupils are not permitted to use their phone throughout the school day
- The sending of abusive or inappropriate messages if forbidden
- Staff should always use a school phone when contacting parents

- Staff, including visitors, volunteers and student teachers, are not permitted to access their phones within the classroom or corridors and these should be switched off and stored away safely during the school day
- Staff may use their mobile phones within the staff room or any of the school offices
- Parents are not permitted to use their mobile phones on the premises or when assisting with a school trip unless permission has been given (school plays for example) and then these pictures should be of their own child only.

Inclusion

Through our use of ICT, we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in our school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through meetings with our SEND Co-ordinator and individual teachers to ensure all children have equal access to ensure success in this subject. Pupils are taught in all lessons to be critically aware of the materials/content they access online and are guided to validate the accuracy of inform.

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding and so concerns must be handled in the same way as any other safeguarding concern. Safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should speak to the safeguarding lead with any concerns (no matter how small these seem) to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom.

School procedures for dealing with online safety will be mostly detailed in the following policies:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

Schools in Oak Learning Trust commit to take all reasonable precautions to safeguard pupils online but recognise that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the designated safeguarding lead as soon as possible on the same day. The reporting member of staff will ensure that a record is made of the concern on CPOMS - this includes any concerns raised by the filtering and monitoring systems.

Any concern/allegation about staff misuse is always (similar to any safeguarding concern) referred directly to the DSL/DDSL, unless the concern is about the Headteacher/Head of School, in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the Whistleblowing policy.

The school will actively seek support from other agencies as needed (i.e. the local authority, Clennell, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2024 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 31-33 for guidance on child-on-child sexual violence and harassment, behaviour incidents online and mobile phones.

The school will inform parents/carers of online safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law.

The school should ensure all online safety reporting procedures are sustainable for any unforeseen periods of closure.

There are various types of online incidents which are deemed as causing a concern and are priority areas:

Nudes – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings.

Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

It is important that everyone understands that whilst the sharing of nudes involving children is illegal, students should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.

The school DSL will use the full guidance document, 'Sharing nudes and semi-nudes' advice for educational settings to decide next steps and whether other agencies need to be involved and next steps regarding liaising with parents and supporting pupils.

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child-on-child abuse pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Cyberbullying

Online bullying (which may also be referred to as cyberbullying), including incidents that take place outside of school should be treated like any other form of bullying and the school bullying policy should be followed. This includes issues arising from banter.

It is important to be aware that sometimes fights are being filmed, live streamed or shared online and fake profiles are used to bully children in the name of others. When considering bullying, staff will be reminded of these issues.

Child-on-child sexual violence and sexual harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the guidance in KCSIE. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language. This will be discussed in staff training.

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 the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

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/handbook.

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.

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.

Social media incidents

Social media incidents involving pupils are often safeguarding concerns and should be treated as such and staff should follow the safeguarding policy.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff). See the social media section later in this document for rules and expectations of behaviour for children and adults in the community.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community (e.g. parent or visitor), will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

Data protection and cyber security

It is important to remember that there is a close relationship between both data protection and cyber security and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cyber Security for Schools and Colleges.

Schools should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2024, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Appropriate filtering and monitoring

The DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" states:

> "It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their

school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified…"

The designated safeguarding lead has lead responsibility for filtering and monitoring and works closely with OneIT to implement the DfE filtering and monitoring standards, which require schools to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs.

We look to provide 'appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times.

We ensure ALL STAFF are aware of filtering and monitoring systems and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking. They can submit concerns at any point via CPOMS and will be asked for feedback at the time of the regular checks.

Technical and safeguarding colleagues work together closely to carry out annual reviews and check and also to ensure that the school responds to issues and integrates with the curriculum.

We carry out half-termly checks to ensure all systems are in operation, functioning as expected, etc and an annual review as part of an online safety audit of strategy, approach etc.

Securly is enforced on any accessible search engines on all devices.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out.

The DSL checks filtering reports and notifications as necessary and takes any necessary action as a result.

According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access

- individual device monitoring through software or third-party services

Monitoring alerts are checked when sent to DSL/DDSL

Acceptable Use

The internet is a valuable resource that can raise educational standards by offering both pupils and teachers opportunities to search for information from a very wide range of sources based throughout the world. The school has a duty to ensure that before using the internet with pupils, staff have had the opportunity to discuss how they will deal sensitively with inappropriate use.

Oak Learning Trust aims to:

- ensure pupils, staff, trustees, governors and visitors will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- offer guidelines which safeguard and protect pupils and all adults from misuse of technology.
- ensure that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- ensure staff are protected from potential risk in their use of ICT in their everyday work.

All stakeholders that access technology and the internet read and sign an acceptable use agreement document at the start of each academic year. Copies can be located in the appendix of this policy.

Messaging/commenting systems

Staff within Oak Learning Trust use the email system provided by Microsoft Outlook for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system.

Staff also use Parentpay, Seesaw, Class Dojo, Facebook, School website to communicate with parents.

Any systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform or app with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from, or data being uploaded to the wrong account. If this a private account is used for communication or to store data by mistake, the DSL/Headteacher/Head of School (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Appropriate behaviour is expected at all times, and any system or app should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher/Head of School and Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations.

Where staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited, and material only used with permission.

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For social media
- For a specific high-profile image for display or publication

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. Members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services (NB – many phones automatically back up photos and these must be deleted).

Photos are stored on Teams in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded at the start of the academic year and whenever appropriate about the importance of not sharing images on social media or otherwise without permission, due to reasons of child protection (e.g. children who are looked after by the local authority may have restrictions in place for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children.

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social media

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first searching online about the school, and the Ofsted pre-inspection check includes monitoring what is being said online.

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 but the school regularly deals with issues arising on social media involving pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Although the school has an official Facebook account and will respond to general enquiries about the school, it asks parents/carers not to use these channels, especially not to communicate about their children.

Email is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

Pupils are not allowed to be 'friends' with or make a friend request to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) as laid out in the AUPs. However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there has been a considerable number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on **Error! Reference source not found.** and permission is sought before uploading photographs, videos or any other information about other people. Parents must **not** covertly film or make recordings of any interactions with pupils or adults in schools or near the school gates, nor share images of other people's children on social media as there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of children for internal purposes such as recording attainment, but it will only do so publicly if parents have given consent on the relevant form.

Use of school devices

Staff and pupils are expected to follow the terms of the school acceptable use policies for appropriate use and behaviour when on school devices, whether on site or at home.

School devices are not to be used in any way which contravenes AUPs, behaviour policy / staff code of conduct.

Wi-Fi is accessible to staff for school-related internet use and for visiting adults as appropriate. All such use is monitored.

School devices for staff or students are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning.

All and any usage of devices and/or systems and platforms may be tracked.

Searching and confiscating

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher/Head of School and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendix 1 – ICT Acceptable Use Agreement Staff, Trustees, Governors and Visitors

ICT Acceptable Use Agreement Staff, Trustees, Governors and Visitors

Digital technologies have become integral to the lives of children and young people, both within school and outside of school. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people have an entitlement to safe internet access at all times, and therefore the purpose of this is to ensure they are responsible and safe while using the internet and other digital technologies for educational use.

Acceptable Use of the ICT systems and Internet: Agreement for all adults in school

- I understand that I must use school computing systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the computing systems and other users.

This Acceptable Use agreement is intended to ensure:

• that staff, trustees, governors and visitors will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

• that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk

• that staff are protected from potential risk in their use of technology in their everyday work. The school will try to ensure that staff, governors and visitors will have good access to digital technology to enhance their work, to enhance learning opportunities for learners, and will, in return, expect staff, governors and visitors to agree to be responsible users.

For my professional and personal safety:

• I understand that the school will monitor my use of the school digital technology and communications systems.

• I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.

• I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

• I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

• I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

• I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

• I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

• I will ensure that when I take and/or publish images of others I will do so with their permission. I will not use my personal mobile phone/smart watch to record these images, unless I have permission to do so.

• I will only use social networking sites in school in accordance with the school's policies.

• I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner. (I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and Oak Learning Trust have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

School will ensure that staff receive online safety training as part of their induction and that ongoing online safety training and updates will be integrated, aligned and considered as part of schools' overarching safeguarding approach. This includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

• When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
• I will not use personal email addresses on the school system.
• I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
• I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
• I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
• I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
• I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School's Data Policy.
• I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
• I will immediately report any damage or faults involving equipment or software, however this may have happened.

I understand that I am responsible for my actions in and out of the school:
• I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
• I understand that if I fail to comply with this acceptable use agreement that action may be taking in line with the school's Disciplinary Policy. In the event of illegal activities, the police will be notified.
I have read and understand the above and agree to use the schools digital technology systems, both in and out of school, and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name (print):	**Name (signed):**
Role	**Date:**

Appendix 2 – ICT Acceptable Use Agreement Foundation/Key Stage 1

ICT Acceptable Use Agreement Foundation/Key Stage 1

Digital technologies have become integral to the lives of children and young people, both within school and outside of school. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people have an entitlement to safe internet access at all times, and therefore the purpose of this is to ensure they are responsible and safe while using the internet and other digital technologies for educational use.

<table>
<tr><td colspan="2">Acceptable Use of the ICT systems and Internet: Agreement for pupils and parent/carers.</td></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">• I will ask a teacher or suitable adult if I want to use the computers/tablets/iPad.
• I will only use activities that a teacher or suitable adult has told or allowed me to use.
• I will take care of computers/tablets/iPad and other equipment.
• I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
• I will tell a teacher or suitable adult if I see something that upsets me on the screen.
• I know that if I break the rules, I might not be allowed to use a computer/tablet/iPad.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/Carer Agreement:
I agree that my child can use the ICT systems and Internet when appropriately supervised by a member of staff. I agree to the conditions above and will make sure my child understands these when using the ICT systems, Internet and using personal electronic devices.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

Appendix 2 – ICT Acceptable Use Agreement Key Stage 2

ICT Acceptable Use Agreement Key Stage 2

Digital technologies have become integral to the lives of children and young people, both within school and outside of school. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people have an entitlement to safe internet access at all times, and therefore the purpose of this is to ensure they are responsible and safe while using the internet and other digital technologies for educational use.

Acceptable Use of the ICT systems and Internet: Agreement for pupils and parent/carers.	
Name of pupil:	
• I will only use websites, applications or devices that a teacher or suitable adult has told or allowed me to use. • I will take care of the computer and other equipment. • I will use any devices, websites or applications (including internet, email, digital video, mobile technologies) for school work only. • I understand that I must use the school ICT systems in a responsible way to ensure there is no risk to my safety or the safety and security of the ICT systems or others. • I will not try to upload, download or access materials that are illegal, inappropriate or cause harm. • I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong. • I will use the username/password I have been given but I will not share my password with anyone, including my friends. • I will never give personal information (name, address, telephone numbers) to anyone without permission of my teacher/parent/carer. • I will be kind to others, not being rude or making them upset. • I will respect others' work and property, including taking or distributing images without permission. • I must listen carefully to my instructions to know about saving my work, logging off and using the printers. • I will tell my teacher immediately if: -I click on a website by mistake. -I receive messages from people I do not know (I will be aware of "stranger danger" when online. -I find anything that may upset or harm me or my friends. -I think there is fault damage or fault with equipment or software. • I will not use the school systems or devices for online gaming, file sharing or video broadcasting (e.g. YouTube), unless I have had permission to do so. I will not any social media sites within school at any time. • I know that if I break the rules, I might not be allowed to use the devices. • When I am using the Internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me. I should make sure that I have permission to use the original work in my own. • I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information). • I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to appropriate action. This may include loss of access to the school network/internet, contact with parents and in the event of illegal activities involvement of the police.	
Signed (pupil):	Date:
Parent/Carer Agreement: I agree that my child can use the ICT systems and Internet when appropriately supervised by a member of staff. I agree to the conditions above and will make sure my child understands these when using the ICT systems, Internet and using personal electronic devices.	
Signed (parent/carer):	Date: