Oakdene Primary School

in association with

St.Helens Council

Online Safety Policy
Inc Social Media Policy

Policy Adapted by: M.Weston

Date reviewed: July 2023
Date to be reviewed: July 2025

Growing and Learning Together

1. Aims

Oakdene Primary School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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

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

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and Responsibilities

3.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing our whole school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

- The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Head Teacher and Deputy Head Teacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority disciplinary procedures).
- The Head Teacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head Teacher and Senior Leaders will ensure those in school who carry out the internal online safety monitoring are also monitored and supported.
- The Senior Leadership Team will receive regular monitoring reports from the Computing Subject Leader.

From September 2023, the headteacher is Mrs Lynsey Young.

3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The designated Safeguarding lead is currently Mr Martin Weston (Deputy Head Teacher). The deputy Safeguarding leads are Mrs Caroline Hughes (Assistant Head Teacher) and Mrs Andrea Green (Pastoral Lead).

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, local authority IT staff, and other school staff (as necessary), to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged on the school CPOMS system and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMS and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety. The school subscribes to National Online Safety website for access to regular training.
- Liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

The Designated Safeguarding Lead/Child Protection Lead should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding 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

3.4 The Computing Subject Leader

The Computing subject leader has the following responsibilities:

- Consults regularly with other members of the school community (e.g. pupils through pupil voice; parents through surveys and internet safety workshops) to ensure knowledge and application of online safety is current.
- Takes day-to-day responsibility for online safety issues and has the leading role in establishing and reviewing the school online safety policies
- Ensures that all staff be aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Maps and ensures provision of the online safety curriculum provision throughout school (yearly planning from Knowsley Computing Scheme being used currently).
- Contributes to relevant and up-to-date training and advice for staff in INSET, reports to the governing body (in liaison with the DSL) and any workshops for parents
- Liaises with school technical staff & school office staff, and reports to the headteacher

3.5 The IT Technician

The IT Technician allocated to Oakdene by the local authority has the following responsibilities (in liaison with the Computing subject leader and office manager):

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a half-termly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files. Education broadband connectivity is provided through St Helens IT. Smoothwall is used for filtering and this is reviewed centrally by St Helens IT. Smoothwall blocks any sites deemed unsuitable for use by children in school.

3.6 Teaching and support staff

All school staff have the following responsibilities:

- Maintaining an understanding of this policy and implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the behaviour policy
- Ensuring they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices.
- Communicating with pupils, parents or carers on a professional level and only carried out using official school systems (e.g. Class Dojo or school email address for communication with parents).
- Ensuring online safety issues are embedded in all aspects of the curriculum delivery. From Autumn 2020, Knowsley Computing Scheme has been used to inform teaching content of online safety.
- Enabling pupils to understand and follow the Online Safety Policy and Internet Use Policy for Pupils (see Appendix 1).
- Enabling pupils to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (taught within the Computing curriculum as part of Digital Literacy).
- Monitoring the use of digital technologies in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

3.7 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
- Support the school in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events – a form will be signed to declare that any images will not be used inappropriately for social media/sharing etc.
- Access parents' sections of the school website sensibly and appropriately
- Ensure appropriate responses on school social media platforms – Facebook and Twitter – as well as our Class Dojo system to communicate with staff, or email communication with the school office

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

Supply teachers are given a specific supply teacher log-in and password and access to a laptop when they are teaching at Oakdene. This gives them access to necessary planning on the school system.

3.9 Pupils

The following applies to all pupils at Oakdene:

- They are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- They gain a good understanding of research skills and realise the need to avoid plagiarism and uphold copyright regulations
- They understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- They will be expected to know and understand policies on the taking / use of images and on different aspects of cyber-bullying.
- They understand the importance of adopting good online safety practice when using digital technologies out of school and realise that this policy covers their actions out of school, if related to their membership of the school.
- Should they see something on their screen that they deem to be inappropriate, they turn off their screen and alert a member of staff immediately.
- They learn about logging on and the importance of keeping passwords safe and secure, not sharing their details with others, and use this in their Computing work both inside and outside of school.

4. Educating pupils about online safety
Pupils will be taught about online safety as part of the Computing curriculum:

All schools also have to teach:

- Relationships education and health education in primary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited. From autumn 2020, this has been through the Knowsley Computing subscription service, which provides a set of lessons for every year group on digital literacy and which is regularly updated to include the most relevant content.

- All children at Oakdene learn about online safety during the autumn term of each year group. All children complete a Digital Literacy unit, which focuses heavily on online safety. This is done using resources from the Knowsley Scheme for Learning. More information can be found in our Computing at Oakdene statement.
- We have a focus on internet safety around Safer Internet Day in the spring term each year.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and activities.
- Pupils should be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school, including keeping their log-in details and passwords safe and not sharing them with others.
- Staff should act as good role models in their use of digital technologies and the internet.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5.1 Educating parents about online safety

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet in an appropriate way. The school will take every opportunity to help parents understand these issues through regular updates through the school website. These updates should inform them of relevant and up-to-date national online safety campaigns, literature and issues. Further newsletters, letters and workshops will be arranged as necessary to supplement the information on the website.

The school will raise parents' awareness of internet safety via communications home on Class Dojo, and in information via our website. This policy will also be shared with parents on the school website.

Online safety is covered during back-to-school meetings with parents at the start of each academic year.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

5.2 Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community.

5.3 Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff via staff inset sessions. This will be regularly updated and reinforced. An audit of the online safety training needs will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school / academy Online Safety Policy and Acceptable Use Agreements.
- Some staff may identify online safety as a training need within the performance management process.
- The Computing subject leader will receive regular updates through attendance at external training events (e.g from Knowsley Computing Conferences or St Helens subject leader training) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to staff.
- The Online Safety Lead will provide further guidance or training to individuals as required. Additional training may be given to staff via the National College training subscription service used in school.

5.4 Education & Training – Governors

Governors / Directors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee involved in technology, online safety, health and safety or safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisations
- Participation in school information sessions for staff or parents
- Updates as required in governors meetings related to important changes to online safety
- Access to training via the National College online training units

6 Technical – infrastructure / equipment, filtering and monitoring

The school technician, in conjunction with the school and local authority, will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible, and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- 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 personal log-in and password to access the school server and emails.
- For the school website and other subscription services, users will be provided with an individual username and password (provided by the Computing subject leader). Users are responsible for the security of their username and password and should alert staff if they feel the security of their log-in information has been compromised.
- The office manager, technician and Computing subject leader are responsible for liaising and ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (e.g. when apps have been purchased).
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- 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.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems. A supply teacher log-in enables supply staff to access teaching plans on the school server.
- Teachers and office staff have access to allocated school devices (laptops and iPads). Staff members should not download and install executable files or programmes/apps on school devices. This should be raised as a request to the school technician via either the School IT Portal, via email, or by speaking to the technician on his designated day inn school. The exception to this policy is for free apps which can be installed on to staff iPads using Apple log-ins via the Apple store, as long as their purpose is educational.
- When working off-site, staff members can access files via Teams or via Cloud sync. They should use Forticlient to access the school network remotely on their devices for services such as SIMS or printing. One Drive may also be used for file storage.
- Any pen drives/memory sticks used must be encrypted and password protected. Personal data cannot be sent over the internet or taken off the school site. It is highly recommended that pen drives and memory sticks are not used in school.

6.2 Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include cloud based services such as email and data storage. All users should understand that the primary purpose of mobile devices in a school context is educational.

The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*[2]	*Yes*[2]
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only				*No*	*No*	*No*

School-owned laptops and tablets (iPads) are allocated to teaching staff members, as outlined in the technical section above. The usage of these devices is outlined in the section below (Internet Use).

6.3 Internet Use

The following rules must be adhered to when using the internet in school:

- Internet access is provided to schools through the St Helens school broadband. This infrastructure provides an Internet firewall and a filtering mechanism, presently installed at either school or LEA level. Members of staff should not attempt to circumvent or disable any of these features.
- Members of staff should use their individual username and password when accessing the Internet and should not allow other staff to use their usernames.
- When logged onto their Internet account, members of staff should not leave a workstation unattended unless it is locked. This can be done using Windows + L keys.
- All connections to the Internet, from within school, must be made through the school network.
- Members of staff should not use, or try to use, a school Internet account for intentionally accessing, displaying, storing or transmitting material that is obscene, sexually explicit, pornographic, racist, defamatory, hateful, incites or depicts violence, or describes techniques for criminal or terrorist acts or otherwise represents values which are contrary to School policy.

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

[2] These devices are not allowed in classrooms and should only be kept and used in the staff room or outside the school building unless express permission has been granted by the head teacher or other senior leader in exceptional circumstances.

- Where access to such sites occurs accidentally this should be immediately reported to the Head Teacher, DSL or Computing Subject Lead.
- Only those members of staff who are duly authorised by the Governing Body may publish content on electronic forums, upload software or data belonging to the School (e.g. school website, school Twitter account). Currently, all teachers can post content onto Twitter, whilst Facebook content is handled by Mr Weston. All staff have access to Class Dojo, with access managed by the school business manager.
- The downloading or purchase of software must be subject to prior authorisation, and in accordance with the school's financial regulations. All software should be properly licensed and registered.
- The downloading of entertainment software, games, music or screen savers (other than for legitimate teaching purposes) is not allowed. Where legitimate downloading takes place it must not breach the rights of copyright owners.
- Any orders placed via the Internet must first be authorised through the normal school financial procedures and in accordance with Financial Regulations.
- The playing of games against an opponent via the Internet is forbidden unless it forms part of a school-purchased educational app (e.g. TT Rockstars).
- Users should not use, or try to use, the Internet to break through security controls (i.e. hacking).
- Users should not do anything which is illegal under English law or the law of any other relevant country.
- Users should not use, or try to use, a Council/School Internet account for political lobbying.
- Users should not use, or try to use, the Internet to intentionally access or transmit computer viruses or similar software.
- Any software or files downloaded via the Internet becomes the property of the School.
- E-mail users have a duty of care to protect the School, in accordance with the Code of Conduct, from any legal action for the likes of defamation, harassment, libel etc. resulting from staff use of the system.
- Care should be taken when in receipt of unsolicited e-mail as it could be a vehicle for introducing viruses.
- Care must be taken over the content of e-mails. It is important that the inclusion of personal information and of personal references to pupils should be avoided wherever possible. Under Data Protection Legislation, in the event of a Subject Access Request, personal data stored on e-mail is classed as relevant data and must be disclosed to the data subject. The word CONFIDENTIAL should be used in the subject box of emails for any necessary correspondence.
- In exceptional cases, where personal data is transmitted, appropriate security measures must be used (eg. Encryption). The St Helens Schools ICT Service can advise schools of the most appropriate method. All e-mails will carry the following disclaimer.
  'This e-mail and any file transmitted with it are confidential, subject to copyright and intended solely for the use of the individual or entity to whom they are addressed. It may contain privileged information. Any unauthorised review, use, disclosure, distribution or publication is prohibited. If you have received this e-mail in error please contact the sender by reply e-mail and destroy and delete the message and all copies from your computer.'

Members of staff are only allowed private use of the Internet in schools if permission has been granted by the Head Teacher. The basis for such use is that:

- All usage is governed by this Policy as outlined in section 6.3
- Access must be in the individual's own time and not in school time.

- Personal use must be confined to viewing or browsing. There must be no storage of information, images, software etc.
- There must be no private interaction (e.g. shopping, entering competitions, use of credit cards, financial services etc).
- If permission is granted to send private e-mails using the 'sthelens.org.uk' accounts then they should be clearly labelled as being private and not being sent as an official communication from and on behalf of the Council/School. The Council/School will not be held responsible for any fraudulent actions.

Teachers in school are allocated school devices (a laptop and an iPad) which can be taken out of school. It is recognised that when using such school laptops and tablets within their own home, staff will have greater freedom in relation to activities such as on-line shopping. When members of staff are using such equipment for personal use at home the following rules apply:

- Members of staff should not use, or try to use, the Internet for intentionally accessing, displaying, storing or transmitting material that is obscene, sexually explicit, pornographic, racist, defamatory, hateful, incites or depicts violence, or describes techniques for criminal or terrorist acts or otherwise represents values which are contrary to School policy.
- Where access to such sites occurs accidentally this should be reported to the Head Teacher, DSL or Computing Subject Leader as soon as possible.
- Members of staff must be aware of, and abide by, current data regulations (GDPR) as its provisions cover data transmitted and stored on e-mail. (See the Data Protection Policy and Code of Practice for further details).
- Only those members of staff who are duly authorised by the governing body may publish school content on electronic forums or upload software or data belonging to the School (e.g. web pages, application data).
- Any downloaded software should be properly licensed and registered. The downloading of music or data must not breach the rights of copyright owners.
- Users should not use, or try to use, the Internet to break through security controls (i.e. hacking).
- Users should not do anything which is illegal under English law or the law of any other relevant country.
- Users should not use, or try to use, the Internet to intentionally access or transmit computer viruses or similar software.
- Only the member of staff to whom the computer has been loaned may use the computer to access the Internet. Allowing other family members or friends to use school equipment to access the Internet is not allowed.

Monitoring of internet usage

Members of staff should be aware that Internet access in school is logged by the filtering system (Smoothwall Safeguarding) and that logs indicating the number and types of web sites that have been accessed by members of staff are subject to review by the Head Teachers and senior leaders. Members of staff using school equipment to access the Internet at home should be aware that the Council's Audit team will, from time to time, make requests for computer equipment to be made available to them for analysis/investigation. Members of staff should be aware that this will not just occur when inappropriate use has been proved, or is suspected but on a random basis. Members of staff should be aware that all Internet activity, using the 'sthelens.org.uk' e-mail accounts, are constantly monitored for inappropriate language. Use of other e-mail accounts will be monitored through random sampling as outlined in the paragraph above. Any inappropriate access/attempts to access, or e-mail activity will be

investigated and may lead to disciplinary action being taken against members of staff. Disciplinary action may take the form of Gross Misconduct/Misconduct depending on the severity of the breach of the policy. Any inappropriate access of a criminal nature will be reported to the Police, or any other relevant agencies that the LEA deems appropriate.

6.4 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press.
- In accordance with guidance from the Information Commissioner's Office, parents/ carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy, and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital images. In these cases, parents are asked to sign a form.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupils' work can only be published with the permission of the pupil and parents or carers.

7 Data Protection

GDPR provides 8 main rights for individuals and strengthens those that already exist under the current Data Protection Act 1998.

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights related to automated decision making and profiling

Personal data will be recorded, processed, transferred and made available according to GDPR 2018 which states that personal data must be:

- Accessed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purpose it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the 'Privacy Notice' and lawfully processed in accordance with the 'Conditions for Processing'
- It has a Data Protection Policy
- It appoints a Data Protection Officer
- It is registered as a Data Controller for the purposes of GDPR
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- A data protection impact assessment (DPIA) will: a) be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy; b) allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur; c) be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices. When personal data is stored on any portable computer system, memory stick or any other removable media:
- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

8 Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their disadvantages:

	Staff & other adults				**Pupils**			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school		X						X
Use of mobile phones in lessons				X				X
Use of mobile phones in social time		X						X
Taking photos on mobile phones / cameras				X				X
Use of school mobile devices e.g. tablets	X						X	
Use of school email for personal emails			X					X
Use of messaging apps		X						X
Use of social media		X						X

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / pupils or parents / carers (email, social media etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. It is recommended that the school email address is used when communicating with a parent via email. Personal email addresses, text messaging or social media must not be used for these communications unless strictly necessary (e.g. contacting a parent on a residential visit in an emergency).
- Pupils can have an email address through Office365 provided by the Schools ICT Service to support with any necessary remote learning. These can be used as part of Computing lessons in school (e.g. using PowerPoint, Excel, Word through Office 365).
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website.

Children are not allowed mobile phones or other electronic devices in school. If they bring one in (e.g. to be safe when walking home), it should be sent to the school office immediately when the children arrive at school and be collected at 3:15 pm from the school office prior to going home.

If children bring phones to after-school events (e.g. discos), they will be collected in and stored safely in the school office until the end of the event. At events where all parents are present (e.g. barbeques), this cannot be instigated but all parents are responsible for the content on their children's devices and will not bring the school into disrepute.

9. Cyber-bullying

9.1 Definition

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

9.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes as part of the curriculum content. The Computing subject leader will also deliver an assembly at least annually linked to Safer Internet Day.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also provides information on cyber-bullying to parents via the school website so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Child-On-Child Abuse

Sexual violence and sexual harassment can occur between two children of any age and sex, including those of primary school age. They can occur online and face to face (both physically and verbally) and are never acceptable. All staff working with children are advised to maintain an attitude of 'it could happen here.'

Any reported instances of child on child sexual violence or harassment must be reported to the DSL and dealt with in accordance with the safeguarding policy. Should any images be recorded on internet enabled devices, staff should always avoid viewing them as to do so would be a criminal offense.

Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. These include, but are not limited to; unauthorised access to school computers; or making, supplying or obtaining malware with the intent to damage the school network.

Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the Cyber Choices programme. This is a nationwide 17 police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

9.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher as per the school behaviour policy, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence
- Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or DSL
- Wherever possible, as per the behaviour policy, contact a parent to alert them to the action
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

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

If inappropriate material is found on the device, it is up to the staff member to liaise with the headteacher and/or DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

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

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

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our school behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

10. Dealing with Unacceptable or Inappropriate Use

Oakdene believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X		

Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)			X		
On-line gambling				X	
On-line shopping / commerce				X	
File sharing			X		
Use of social media			X		
Use of messaging apps		X			
Use of video broadcasting e.g. Youtube		X			

10.2 How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in this policy as well as our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. See appendix 4.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. See appendix 5.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes.

See the flowchart (Appendix 3) below for further guidance.

11. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. This is kept on CPOMS.

This policy will be reviewed every 2 years by the Designated Safeguarding Lead due to continuous and rapid changes in technology. At every review, the policy will be shared with the governing board.

12. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Internet Use and Website Use Policy for Children (Appendix 1)
- Social Media Policy (within this Internet Safety policy pages 23-27)
- ICT acceptable usage policy (Appendix 2)

Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or Roblox, and video sharing platforms such as You Tube have social media elements to them.

Oakdene Primary School recognises the numerous benefits and opportunities which a social media presence offers. Staff members are actively encouraged to find creative ways to use social media and pupils are taught about the benefits within the online safety curriculum. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by Oakdene's staff, parents, carers and children.

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements. This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education

The school respects privacy and understands that staff and pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional & Personal Communications

Professional communications are those made through official school channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with pupils are also considered. Staff should only communicate with pupils via the appropriate comment sections on Seesaw, for example if setting and responding to homework, school work or remote learning digitally.

Roles & Responsibilities

Headteacher & SLT

- Facilitating training and guidance on Social Media use.
- Developing and implementing the Social Media policy
- Taking a lead role in investigating any reported incidents.
- Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
- Receive completed applications for Social Media accounts and refuse/approve account creation.

Administrator / Moderator

- Create the account following SLT approval
- Store account details, including passwords securely
- Be involved in monitoring and contributing to the account
- Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)

Staff

- Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
- Attending appropriate training
- Regularly monitoring, updating and managing content he/she has posted via school accounts
- Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. school Twitter account, or Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Current Accounts & Aims

Oakdene currently has the following social media accounts:

Twitter - @OakdeneRainhill – all staff have access to this account. It is used for whole school events, especially those that link to other people/organisations (e.g. local services, authors). Mrs Caroline Hughes is the administrator.

Facebook – Oakdene Primary – Mr Martin Weston and Mrs Evonne Garton-Pope are the school administrators for Facebook. If other staff wish to post, they should do so via communication with these staff members. This is used infrequently now since the school provides updates on Class Dojo.

YouTube – the school has a YouTube account purely for video content for special occasions (e.g. School Carol Concert produced during lockdown made available for Whiston Hospital) that is too large for the school website or Class Dojo. Mr Martin Weston is the school administrator.

Monitoring

School accounts must be monitored regularly and frequently. Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- If a journalist makes contact about posts made using social media, staff must contact the head teacher or other senior leader before responding.
- Unacceptable conduct (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload student pictures online other than via school social media accounts, the school website, Class Dojo or Seesaw. Reference should always be made to the permissions folder for children's images. This is held in the school office.
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Data Protection

Children's names will not appear on any social media post. Images will only be posted if permission has been granted. In group images, children without permission must have their faces blurred or covered.

Personal use of Social Media

Staff Use

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to private social media sites during break/lunch times and only in permissible areas of the school – this is the staff room and school office.

Pupils

- Staff members are not permitted to follow or engage with current or prior pupils/students of the school on any personal social media network account until that pupil has reached adulthood.
- The school's education programme should enable the pupils to be safe and responsible users of social media.

- Pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy.

Parents/Carers

- If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- The school provides information to parents via the school website which supports the safe and positive use of social media.
- Parents/Carers are encouraged to comment or post appropriately about the school on our social media platforms of Twitter and Facebook, as well as on Class Dojo. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

APPENDIX 1

Oakdene Primary School - Internet Use Policy for pupils

I will only access the system with my class login name and password.

I will not access other people's files, or damage their work and data.

I will only use the Internet when I have permission and am supervised by a teacher.

I will use the Internet only for activities and work set by school.

I will only e-mail people my teacher has approved, and not use the Internet for private messages.

I will respect the privacy of others. I will not publish their names, addresses, phone numbers or photographs.

I will not give my home address or telephone number, or arrange to meet someone, through the Internet.

I will not use work from the Internet as if it was my own. I will give credit to the sources of materials included in my work.

I will not try to find or use unacceptable material from the Internet.

I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself.

I will not use school resources to subscribe to any goods or services, nor buy or sell using the Internet.

I will not download software from the Internet unless this is authorised by the teacher.

I will not bring in disks, CD's or electronic data from outside school unless I have been given permission.

I will not send unsuitable emails or comments in blogs. The messages I send will be polite, responsible and signed in my name.

I will not send anonymous messages.

I will not take part in any activity that goes against school rules or government legislation.

I understand that the school may check my computer folder or log-in to school subscription services and may monitor the Internet sites I visit.

Remember that access is a privilege, not a right and that access requires responsibility!

Sanctions
Any breach of this policy may lead to the following sanctions:

1. A temporary or permanent ban on Internet use.

2. Pupils' parents being contacted.

3. Other external agencies being contacted.

Oakdene Primary School
Web Site Policy

1. The Headteacher will have editorial responsibility for the school Web site and will ensure that content is accurate and the quality of presentation is maintained.

2. The Web site will comply with the school's guidelines for publications.

3. There will be no link between photographs and individual pupil information.

4. Only images of pupils in appropriate dress will be used.

5. No personal information relating to pupils will be included on our Web site (e.g. email addresses or phone numbers).

6. The point of contact on the Web site will be the school address, telephone number and email address.

7. Information, work or photographs produced by or relating to pupils will only be used if parental permission has been given.

Name of Child……

Class……..

I will adhere to the School Internet Policy.

Signed (Child)……..

I acknowledge receipt of the Internet and Web site Policy.

Signed (Parent)……..

APPENDIX 2

Policy for Acceptable Usage of ICT by Staff and Volunteers

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

Aims

- To ensure that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- To 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.
- To protect staff from potential risk in their use of ICT in their everyday work.

Broad Guidelines

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other
- digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems
  (laptops, email etc) out of school.

- I understand that the school ICT 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 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 ICT systems**:

- I will not access, copy, remove or otherwise alter any other user's files, without their 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 equipment to record images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school for personal use. Information shared should never compromise the school's duty to provide the highest possible standard of education or bring the school's reputation into distribute. Staff who have genuine concerns about any school matter should follow school current guidelines and policies eg whistle-blowing to resolve issues and not networking sites. Staff should report all contacts through networking sites which may concern them to the headteacher. Examples may include: child below 13 on Facebook requesting to be a friend or inappropriate comments by a parent directed to staff.
- I will only communicate with students / pupils 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 the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school

- I will not use my personal hand held / external devices (laptops / mobile phones / USB devices, tablets etc) in school. I will only use school equipment.. I am aware that I can sign up for Forticlient to access the school server safely from home.
- I will not use personal email addresses on the school ICT systems for pupils personal data.
- I will not open any attachments to emails, unless the source is known and trusted, 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 (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) 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 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, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or student / pupil 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.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (i.e music/videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

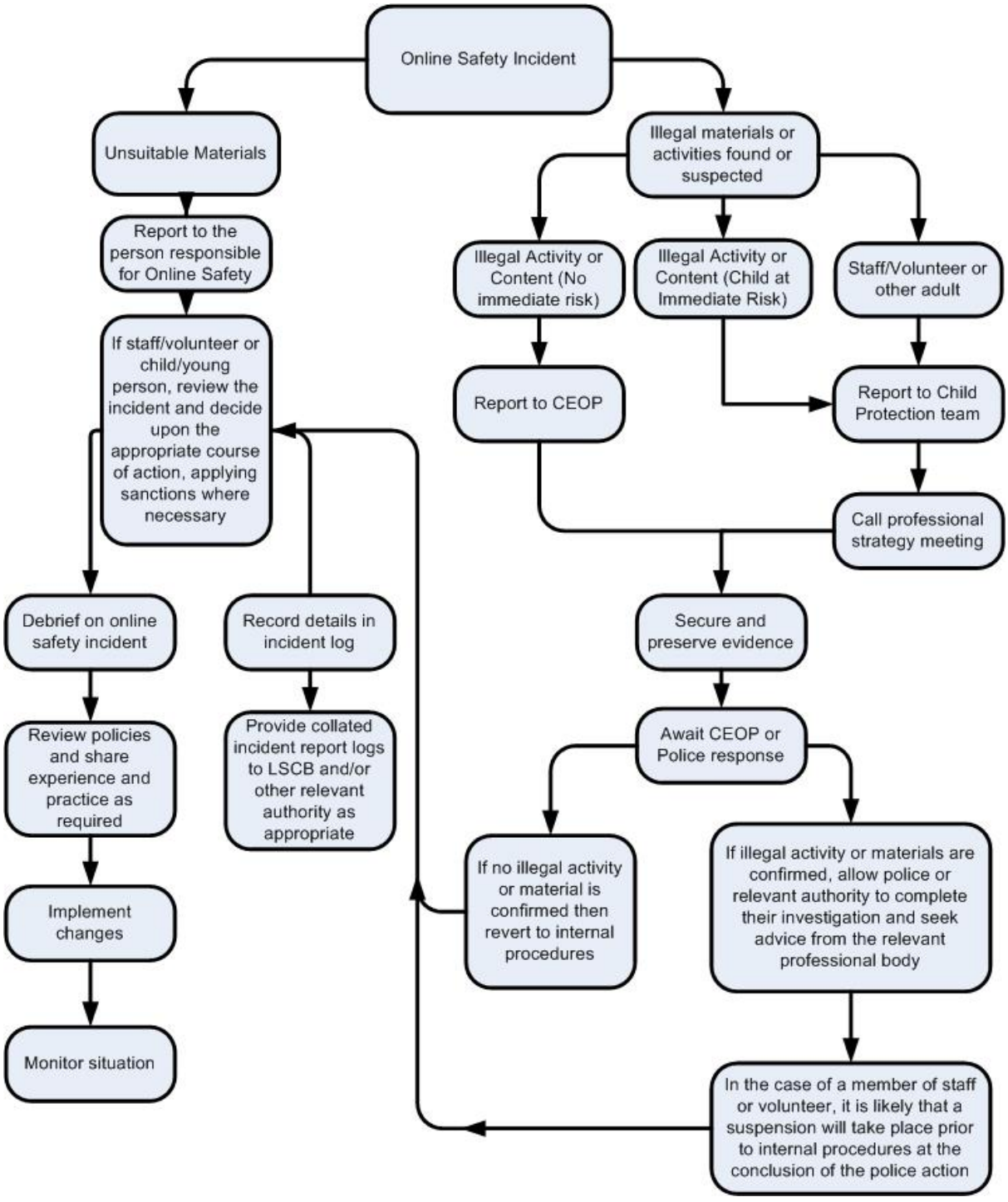
Child Safeguarding Statement

Staff need to ensure that there may be issues relating to a child's behaviour as a result of child protection issues. Where staff have any concerns of this nature the agreed steps outlined in the school's 'Safeguarding' Policy should be followed.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (when carrying out communications related to the school) within these guidelines.

I have signed and dated the Staff sheet which confirms I agree with the Acceptable Use Policy

APPENDIX 3


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

APPENDIX 4 – Guidance for Pupil incidents

Pupil Incidents	CPOMS	Refer to DSL	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Further sanction as per the behaviour policy e.g. reflection
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X				
Unauthorised use of non-educational sites during lessons		X						X
Unauthorised / inappropriate use mobile device	X	X	X			X		X
Unauthorised / inappropriate use of social media / messaging apps / personal email	X					X		X
Unauthorised downloading or uploading of files		X			X			X
Attempting to access or accessing the school network or other educational subscription services, using another pupil's account		X			X	X		X
Attempting to access or accessing the school network, using the account of a member of staff	X	X			X	X		X
Corrupting or destroying the data of other users		X			X	X	X	X
Sending an email or message that is regarded as offensive, harassment or of a bullying nature	X		X			X		X
Continued infringements of the above, following previous warnings or sanctions	X		X	X		X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X		X			X		X

Accidentally accessing offensive or pornographic material and failing to report the incident	X				X	X		X
Deliberately accessing or trying to access offensive or pornographic material	X		X			X	X	X

APPENDIX 5 – Guidance for Staff incidents

Staff Incidents		Refer to Headteacher or Designated Safuegarding Lead	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X		
Inappropriate personal use of the internet / social media / personal email		X				
Unauthorised downloading or uploading of files		X				
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X				
Careless use of personal data e.g. holding or transferring data in an insecure manner		X				
Deliberate actions to breach data protection or network security rules		X				X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X				X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X				
Actions which could compromise the staff member's professional standing		X				
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X				X

Accidentally accessing offensive or pornographic material and failing to report the incident		X				
Deliberately accessing or trying to access offensive or pornographic material		X				X
Breaching copyright or licensing regulations		X				
Continued infringements of the above, following previous warnings or sanctions		X		X		X