



Online Safety Policy

Implementation Date: August 2015
Date / Term of last review: Michaelmas Term 2025

This policy applies to the whole school including those in the EYFS who have access to and are users of the school ICT system, both in and out of the school.

This policy was reviewed and renewal dates updated in line with department developments and budgets.

This policy also includes the following Oakwood policies within its Appendices:

- **Appendix B: IT Acceptable Use Policy**
- **Appendix C: Bring Your Own Device Agreement for Pupils**

Other policies to be read in conjunction with this policy:

- Safeguarding and Child Protection Policy
- Mobile Devices (including Mobile Cameras) Policy for Staff, Governors, Volunteers and Visitors

Author:	Chrissie Zoltowski, DSL Felix Page, Digital Strategy (SMT) Bethany West, Head of IT
Approval:	Clare Bradbury, Headteacher
Next Review Date:	Michaelmas Term 2026

For office use only:

Website	Required	✓
Internal Staff purposes only		

1. Aims and objectives

- 1.1. It is the duty of Oakwood School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for enhanced learning, but also pose great risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse and radicalisation and identity theft.
- 1.2. Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:
 - Websites
 - Email and instant messaging
 - Blogs, forums and chat rooms
 - Mobile internet devices such as smart phones and tablets
 - Social networking sites
 - Music / video downloads
 - Gaming sites and online communities formed via games consoles
 - Instant messaging technology via SMS or social media sites
 - Video calls
 - Podcasting and mobile applications
 - Virtual and augmented reality technology
 - Artificial intelligence
- 1.3. This policy, supported by the IT Acceptable Use Policy (for all staff, visitors and pupils), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:
 - Safeguarding and Child Protection Policy (including KCSIE 2025)
 - Staff Code of Conduct
 - Behaviour Management, Rewards & Sanctions Policy
 - Data Protection Policy and Privacy Notices
 - School Trips Policy
 - PSHE and Well-being Policies
 - Anti-Bullying Policy
 - Mobile Devices (including Mobile Cameras) Policy for Staff, Governors, Volunteers, Visitors
 - Taking, Storing and Using Images of Children Policy
- 1.4. At Oakwood School, we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.
- 1.5. The breadth of issues classified within online safety is considerable. KCSIE 2025 states that digital safety can be categorised into four areas of risk:
 - *Content*: being exposed to illegal, inappropriate or harmful content;

For example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

- *Contact*: being subjected to harmful online interaction with other users;
For example: child to child 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' for example, making sending and receiving explicit images and online bullying; and
- *Commerce*: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If it is felt that pupils or staff are at risk, it should be reported to the Anti-Phishing Working Group. (<https://apwg.org>)

2. Scope of Policy

- 2.1. This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy:
 - "staff" includes teaching and non-teaching staff, governors, and volunteers
 - "parents" includes pupils' carers and guardians
 - "visitors" includes anyone else who comes to the school
- 2.2. Both this policy and our *IT Acceptable Use Policy – Staff, Visitors & Volunteers* (See Appendix B) as signed by staff and pupils, cover both fixed and mobile internet devices provided by the school, (such as PCs, laptops, tablets, webcams, whiteboards, digital recording equipment) and those provided by pupils or visitors (such as personal laptops, watches, smartphones and tablets).
- 2.3. In designing this policy, the school has considered the "4Cs" outlined in KCSIE (content, contact, conduct and commerce) as the key areas of risk. However, the school recognises that many pupils will have unlimited and unrestricted access to the internet via mobile phone networks outside school hours. The improper use of mobile technology by pupils, in or out of school, will be dealt with under the school's Behaviour Management, Rewards & Sanctions Policy and/or Safeguarding and Child Protection Policy as is appropriate in the circumstances.
- 2.4. The School will deal with such incidents as described within this policy and associated Behaviour and Anti-Bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of School.

3. Roles and Responsibilities in relation to online safety

All staff, governors and visitors have responsibilities under the safeguarding policy to protect children from abuse and make appropriate referrals. The following roles and responsibilities must be read in line with the Safeguarding and Child Protection Policy.

The Governing Body

- 3.1. The Governing Body has overall leadership responsibility for safeguarding as outlined in the Safeguarding and Child Protection Policy. The Governing Body of the school is responsible for the approval of this policy and for reviewing its effectiveness at least annually.

- 3.2. The Governing Body will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, to ensure that:
- all staff, in particular the Head of Computing, Digital Development Lead, Network Manager DSL and Senior Leadership Team are adequately trained about online safety
 - all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to escalate concerns when identified
 - staff are aware of the school procedures and policies that should be followed in the event of abuse or suspected breach of online safety in connection to the school
- 3.3. In considering the age ranges of the children (ages 2-11), the number of children (approximately 300) and how often they access the IT systems, the Governing Body will consider the proportionality of costs versus the safeguarding risks. The Governing Body are updated on effectiveness of school filters and monitoring systems in place through regular Education and Safeguarding Committee meetings, ensuring that the leadership team and staff:
- are aware of and understand the systems in place (including languages spoken and terminology)
 - manage them effectively
 - know how to escalate concerns when identified

The Headteacher and the Senior Leadership Team (SLT)

- 3.4. The Headteacher is responsible for the safety of the members of the school community and this includes responsibility for online safety. Together with the Senior Leadership Team, they are responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions at least annually, overseeing reports and ensuring staff are appropriately trained.
- 3.5. In particular, the role of the Headteacher and Senior Leadership Team is to ensure that:
- staff are adequately trained about online safety
 - staff are aware of the school procedures and policies that should be followed in the event of abuse or suspected breach of online safety in connection to the school
 - all members of staff receive regular, up-to-date training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications

The Designated Safeguarding Lead (DSL)

- 3.6. Chrissie Zoltowski is the Designated Safeguarding Lead (DSL) at Oakwood School. The DSL takes the lead responsibility for Safeguarding and Child Protection, which includes responsibility for online safety as well as the school's filtering and monitoring system. The DSL will ensure that this policy is upheld at all times, working with the Headteacher, Senior Leadership Team, Network Manager, Digital Development Lead and Head of Computing to achieve this. As such, in line with the Safeguarding and Child Protection policy, the DSL will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.
- 3.7. The DSL will work closely with the Network Manager, Digital Development Lead and Head of Computing and the school's IT service providers to ensure that the school's requirements for

filtering and monitoring are met and enforced. The DSL will review filtering and monitoring reports and ensure that termly checks are properly made of the system.

- 3.8. The DSL should be trained in online safety issues and be aware of the potential implications for serious child protection/safeguarding issues arising from:
- sharing of personal data
 - access to illegal/inappropriate materials
 - inappropriate contact online with adults/strangers
 - potential or actual incidents of grooming
 - cyber-bullying as facilitated by the technology that then permits any potential child protection issues to arise
- 3.9. The DSL will also:
- act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate
 - ensure all members of staff receive regular, up-to-date and appropriate online safety training
 - access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and that it is up to date to keep pupils safe online
 - keep up-to-date with current research, legislation and trends regarding online safety and communicate this to staff and the wider community as appropriate
 - ensure that online safety is promoted to parents, carers and the wider community through a variety of channels and approaches
 - maintain records of online safety concerns, as well as actions taken, as part of the school's safeguarding recording mechanisms, potentially identifying trends/gaps and updating the educational response to such incidents
 - report online safety concerns, as appropriate, to the Senior Leadership Team and Governing Body
 - review and update online safety policies, acceptable use policies and other procedures on a regular basis (at least annually) with stakeholder input
 - meet regularly with the Designated Safeguarding Governor with lead responsibility for safeguarding and online safety

The Deputy Designated Safeguarding Lead (DDSL)

- 3.10. Gemma Halford is the Deputy Designated Safeguarding Lead (DDSL) who supports the DSL in all online safety matters and acts in their absence.

On Line Safety Coordinators

- 3.11. The DSL has delegated day-to-day responsibilities relating to online safety to the Network Manager (Paul Cooke), Head of Digital Development (Felix Page) and Head of Computing (Beth West). They will keep up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education (including KCSIE), ISI, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Children Procedures. The Network Manager, Digital Development Lead and Head of Computing will share any disclosure, report or suspicion of improper use of school IT or any issues with the school's filtering and monitoring system with the DSL.

- 3.12. In addition, the Network Manager, Head of Digital Development and Head of Computing
- ensure that alongside the DSL, all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
 - receive reports of online safety incidents and creates a log of incidents to inform future online safety developments
 - report, when necessary, to the Senior Leadership Team
 - checks once per term that the filtering and monitoring systems are operating effectively, recording these checks along with any appropriate action

The IT Network Manager and Head of Digital Development

3.13. The school's IT Network Manager and Head of Digital Development have key roles in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage. The IT Network Manager and Head of Digital Development meet weekly to monitor and review systems.

- 3.14. The IT Network Manager and Head of Digital Development will:
- be responsible for the IT infrastructure and ensure it is not open to misuse or malicious attack
 - ensure that users may only access the networks and devices through enforced strong password protection
 - keep up to date with online safety technical information in order to carry out their role
 - ensure that the use of the network (including internet, virtual learning, email and remote access) is monitored for misuse
 - implement any agreed monitoring software/systems
 - ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the school community and ensure that the filtering and the school network system is actively monitored. Any issues, deliberate or accidental, should be reported to the DSL and a log maintained with appropriate action being taken as necessary
 - ensure that appropriate anti-virus software and system updates are installed and maintained on all school machines and portable devices
 - liaise with the DSL to ensure regular audit of monitoring and filtering systems, in line with KCSIE 2025.

Head of Computing

3.15. The Head of Computing takes responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents.

Teaching and Support Staff

3.16. All staff are required to sign and return the IT Acceptable Use Policy before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a

talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

- 3.17. All staff must read and understand this Online Safety Policy and enforce it in accordance with direction from the DSL and the Headteacher/Senior Leadership Team as appropriate.
- 3.18. Teaching and support staff have a responsibility to ensure that during the delivery of the teaching and learning curriculum, online safety is recognised as a key priority. Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. Staff are familiar with what to do in the event of misuse of technology by any member of the school community.
- 3.19. In addition, teaching and support staff:
 - maintain awareness of school online safety policies and practices, knowing when and how to escalate online safety issues
 - report any suspected misuse or problem to the Headteacher or DSL
 - ensure that all digital communications with pupils/parents/carers/fellow staff are on a professional level and are only conducted using school systems
 - ensure pupils understand and follow online safety policies, including the need to avoid plagiarism and uphold copyright regulations
 - ensure that pupils follow the acceptable use policy
 - monitor the use of digital technologies (including mobile devices, cameras etc.) during school activities
 - ensure that where the use of the internet is pre-planned, pupils are 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
- 3.20. In accordance with the Safeguarding and Child Protection Policy, if there is a safeguarding concern a report must be made by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the school's DSL.

Pupils

- 3.21. Pupils are responsible for using the school IT systems in accordance with the IT Acceptable Use Policy, and for letting staff know if they see IT systems being misused.
- 3.22. It is the responsibility of pupils (at a level appropriate to their age and ability) to:
 - use school digital technology systems in accordance with the school acceptable use policy
 - understand and follow online safety policies, including the need to avoid plagiarism and uphold copyright regulations
 - keep themselves and others safe online
 - respect the feelings and rights of others both on and offline, in and out of school
 - seek help from a trusted adult and understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
 - understand policies on the use of mobile devices and digital cameras, the taking/using of images and cyber-bullying
 - understand that the online safety policy will include actions outside of school where related to school activities

Parents and Carers

- 3.23. Oakwood School believes that it is essential for parents to be fully involved with promoting online safety both within and outside school. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.
- 3.24. Parents may underestimate the frequency and extent of harmful material their child could be exposed to on the internet and may be unsure of how to respond. In this regard, parents and carers will be encouraged to support the school in promoting good online safety practice and to follow the school's guidelines on:
- digital and video images taken at school events
 - accessing parent portal on the school website
 - understanding that mobile devices are not permitted at school

4. Filtering and Monitoring

In general

- 4.1. Oakwood School Oakwood aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- 4.2. Staff, pupils, parents and visitors should be aware that the school's filtering and monitoring systems apply to all users, all school-owned devices and any device connected to the school's internet server. Deliberate access, or an attempt to access prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Behaviour Management, Rewards & Sanctions Policy, as appropriate.
- 4.3. The Network Manager will check once per term that the filtering and monitoring systems are operating effectively – these checks must be recorded along with any appropriate action. From time to time the Safeguarding and/or Online Safety governor, the DSL, Head of Digital Development and Head of Computing will review the filtering and monitoring system, looking at the records of the checks. Such a review should occur before the beginning of every new academic year, however such reviews should also occur if:
- there is a major safeguarding incident
 - there is a change in working practices
 - any new technology is introduced
- 4.4. The school uses Smoothwall filtering and monitoring software which restricts and monitors content access by both pupils and staff. Pupils and staff are safe from inappropriate and/or terrorist and extremist material when accessing the internet in school. The filtering system blocks internet access to harmful sites and inappropriate content. Illegal content is filtered by Smoothwall by actively employing the Internet Watch Foundation CAIC list. The filtering system will block access to child sexual abuse material, unlawful terrorist content, adult

content, misinformation, disinformation and conspiracy theories, as well as other inappropriate content.

- 4.5. If there is a good educational reason why a particular website, application, or form of content should not be blocked, a pupil should contact the relevant member of teaching staff, who will then contact the Network Manager, Head of Digital Development or Head of Computing and DSL for their consideration.
- 4.6. The school will monitor the activity of all users across all of the school's devices or any device connected to the school's internet server allowing individuals to be identified. In line with the school's Data Protection Policy and Privacy Notices, the Network Manager, Head of Digital Development and Head of Computing and IT Staff will monitor the logs daily. Any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSL immediately. Teaching staff should notify the Network Manager, their Head of Department and the DSL if they are teaching material which might generate unusual internet traffic activity.
- 4.7. The IT Network Manager may view a computer screen at any time without the user's knowledge to ensure the system is being used appropriately.

Staff

- 4.8. If any member of staff has any concern about the effectiveness of the filtering and monitoring system, they must report the matter to the DSL immediately in line with the Safeguarding and Child Protection Policy; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content. If any member of staff accidentally accesses prohibited or otherwise inappropriate content, they should proactively report the matter to the DSL.
- 4.9. While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff should notify the head of their department, Network Manager and the DSL if they believe that appropriate teaching materials are being blocked.

Pupils

- 4.10. Pupils must report any accidental access to materials of a violent or sexual nature or that are otherwise inappropriate to the Network Manager, Head of Digital Development, Head of Computing, DSL or appropriate teacher. Deliberate access to any inappropriate materials by a pupil will be dealt with under the school's Behaviour Management, Rewards & Sanctions Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.
- 4.11. Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work/research purposes, pupils should contact a member of the IT staff and the Network Manager for assistance.

5. Education and Training

Staff Awareness and Training

- 5.1. As part of their induction, all new staff receive information on online safety, including the school's expectations, applicable roles and responsibilities regarding filtering and monitoring. This will include training on this Online Safety Policy.
- 5.2. All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the school's Online Safety procedures. These behaviours are summarised in the IT Acceptable Use Policy which must be signed and returned before use of technologies in school.
- 5.3. All teaching staff receive regular information and training (at least annually) on online safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. All supply staff and contractors receive information about Online Safety as part of their safeguarding briefing on arrival at school.
- 5.4. Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community. When pupils use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.
- 5.5. In accordance with the Safeguarding and Child Protection Policy, if there is a safeguarding concern a report must be made by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the school's DSL.

Pupils: The Teaching of Online safety

- 5.6. Online safety guidance will be given to pupils on a regular basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.
- 5.7. With the explosion in technology, we recognise that blocking and barring sites is no longer adequate. Through our education and training for pupils they begin to understand why they need to behave responsibly if they are to protect themselves.
- 5.8. The school provides opportunities to teach about online safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school is also carried out via PSHE and Well-being lessons, by presentations in assemblies, as well as informally when opportunities arise.
- 5.9. At age-appropriate levels, often via PSHE, Jigsaw and computing lessons, pupils are taught how to research on the internet and to evaluate sources to look after their own online safety. They are educated into the importance of evaluating the intellectual integrity of different sites, and why some apparently authoritative sites need to be treated with caution as some websites that appear to be serious, impartial, historical sites, actually masquerade as sources of racist, homophobic, jihadist or other propaganda. Some free, online encyclopaedias do not evaluate or screen the material posted on them. Pupils learn to develop the skill of knowledge location, retrieval and evaluation. Pupils are taught to be critically aware of the materials they read and are shown how to validate information they have before accepting its accuracy.

- 5.10. At age-appropriate levels, pupils are taught about their online safety responsibilities and to look after their own online safety. From Year 4, pupils are formally taught about recognising online sexual exploitation, stalking and grooming, sexting or youth produced sexual imagery, and of their duty to report any such instances they or their peers come across. Through our PSHE curriculum, pupils are made aware that child-on-child abuse can take the form of cyberbullying and that the school has a zero-tolerance approach to this type of abuse. Pupils can report concerns to the DSL, Network Manager, Head of Digital Development, Head of Computing or any member of staff at the school.
- 5.11. From Year 4, pupils are also taught about relevant laws applicable to using the internet such as those that apply to data protection, online safety and intellectual property. Pupils are taught about respecting other people's information and images through discussion and classroom activities.
- 5.12. Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-Bullying Policy which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the DSL, or any other member of staff they trust, as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.
- 5.13. Pupils are made aware that by logging in to their school Google accounts at school or at home, they have the added protection of the school's online filtering and monitoring systems.
- 5.14. Pupils will prepare their own models of good practice, which form the subject of presentations at assemblies and discussion in the meetings of the School Council. They cover the different hazards on the internet, such as grooming, stalking, abuse, bullying, harassment, upskirting and identity theft. Guidance covers topics such as saving yourself from future embarrassment, explaining that any blog or photograph posted onto the internet is there permanently. Anything that has been deleted may be cached in a search engine, company server or internet archive and cause embarrassment years later.
- 5.15. The whole school takes part in internet safety and awareness days.
- 5.16. Pupils of all ages are encouraged to make use of the excellent online resources and publications that are available from:
- www.swgfl.org.uk
 - www.saferinternet.org.uk
 - www.childnet.com/parent-and-carers
 - www.thinkuknow.co.uk
 - www.common sense media.org
 - www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
 - www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/
 - Digizen (www.digizen.org.uk)
 - Cyber Mentors (www.cybermentors.org.uk)
 - Childnet International (www.childnet-int.org)
 - Cyberbullying (www.cyberbullying.org) or (www.common sense media.org)
 - E-Victims (www.e-victims.org)
 - Bullying UK (www.bullying.co.uk)

Parents

- 5.17. The school seeks to work closely with parents and guardians in promoting a culture of online safety. The school will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.
- 5.18. The school recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school has therefore subscribed to 'Online Safety UK' which provides termly talks at school, newsletters and online sessions for parents to attend. These sessions give advice about online safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.
- 5.19. The school also seeks to inform parents and raise awareness of online safety issues via newsletters, parents' evenings and posting information on the school website and Friday flyers.

6. Use of School and Personal Devices

Staff

- 6.1. School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Devices issued to staff are encrypted to protect data stored on them.
- 6.2. Staff are referred to the Staff and Visitors BYOD Policy (within the Mobile Devices Policy), Staff Code of Conduct and IT Acceptable Use Policy for further guidance on the use of non-school owned electronic devices for work purposes.
- 6.3. Staff at Oakwood School are permitted to bring in personal devices for their own use. Mobile telephones may be used in secure staff locations during break-times and lunchtimes only. Staff are not permitted to have their personal devices switched on or visible during teaching time or when around pupils.
- 6.4. Staff are not permitted under any circumstances to use their personal devices when taking images, videos or other recordings of any pupil nor to have any images, videos or other recording of any pupil on their personal devices. Please read this in conjunction with the Safeguarding and Child Protection Policy, IT Acceptable Use Policy, Staff Code of Conduct, School Trips Policy and Mobile Devices (including Mobile Cameras) Policy for Staff, Governors, Volunteers and Visitors.
- 6.5. Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents/carers and under no circumstances may staff contact a pupil or parent/carer using a personal telephone number, email address, social media, or other messaging system.
- 6.6. Staff wishing to use their own mobile device must sign a Bring Your Own Device (BYOD) statement. Further information and guidance on non-school owned electronic devices can be found in the Staff Policy Handbook and Mobile Devices (including Mobile Cameras) Policy for Staff, Governors, Volunteers and Visitors.

Pupils

- 6.7. At Oakwood School, we believe it is unnecessary for pupils to bring a mobile device onto the school site. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology. Requests, in exceptional circumstances, must be made to the Headteacher in writing, and if approved, the device must be left in a lockable cupboard in the school office and may not be accessed during the school day. Pupils are permitted to bring in 'e-readers' that do not connect to the internet; these will be brought into the school with the agreement of the school and parents and pupils will need to have read and signed the IT Acceptable Use Policy (Appendix B) and Pupil Mobile Device Policy (Appendix C).
- 6.8. School mobile technologies are available for pupil use under staff supervision (including laptops, tablets, cameras, etc.) and are stored in lockable cupboards around the school. Members of staff should use the online booking system to reserve devices and ensure they are returned in good working order.
- 6.9. Pupils are responsible for their conduct when using school-issued devices. Any misuse of devices by pupils will be dealt with under the school's Behaviour Management, Rewards & Sanctions Policy.
- 6.10. The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, where possible they will use a school device (such as a chromebook for extended writing) however where their own devices are needed to be used the SENDCo will create a pupil plan, shared and agreed with parents, to agree how the school can appropriately support such use. This individual plan will be shared with staff to ensure that devices are used appropriately.
- 6.11. Prior to any approved device being brought into school, the pupil and parents will need to read and sign the IT Acceptable Use Policy (Appendix B) and Pupil Mobile Device Policy (Appendix C) and the IT Network Manager will set up the relevant access on the device.
- 6.12. Pupils are always monitored by staff when using the school IT resources.

Use of school and personal devices for pupils on trips and residentials

- 6.13. Pupils are not permitted to take personal devices on school trips, both day and residential, unless specified as part of an individual needs plan. Where a pupil's individual need requires a device to facilitate interventions, a school device will be used wherever possible and under the direction and agreement of the parents, SENDCo and DSL; the use of the device will be overseen by an assigned member of staff on the trip and details will be included in the trip risk assessment, approved by the EVC.
- 6.14. In exceptional circumstances as detailed above, where a reasonable adjustment is required (for example, to support a student's additional needs or specific communication requirements), the school may permit a personal mobile device to be taken on a school trip or residential visit. In these cases, clear measures will be put in place to mitigate any potential misuse, such as:
 - The device is kept by a member of staff except when required for its intended purpose
 - Restrictions on when and how the phone can be used
 - Agreement between parents/carers, staff and the pupil on the expectations for use

- Pupils are not permitted to use the device to take photos or videos under any circumstances
- Any breach of these expectations may result in the withdrawal of the privilege for future trips and will be managed in line with the school's Behaviour Policy.

6.15. On trips that take place outside of term time, such as the annual ski trip, pupils are permitted to take one personal device. This device can only be used under adult supervision and it must not have access to the internet or wifi. Devices will be collected daily and only given to children during adult supervised free time.

7. Online Communications

Staff

- 7.1. Any digital communication between staff and pupils or parents/carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent/carer using any personal email address or SMS/WhatsApp. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business. Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents/carers. Under no circumstances may staff contact a pupil or parent/carer using a personal telephone number, email address, or other messaging system nor should pupils or parents/carers be added as social network 'friends' or similar.
- 7.2. Staff must immediately report to the DSL or Headteacher 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. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the Network Manager or IT Staff.
- 7.3. The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored. Staff should only use their school email address to communicate with parents and other members of staff or to discuss school related communications.
- 7.4. Any online communications must not either knowingly or recklessly:
- place a child or young person at risk of harm, or cause actual harm
 - bring Oakwood School into disrepute
 - breach confidentiality
 - breach copyright
 - breach data protection legislation
 - do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
 - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age
 - using social media to bully another individual
 - posting links to or endorsing material which is discriminatory or offensive

- 7.5. Where communication is received that makes a member of staff uncomfortable, is offensive (including 'banter'), discriminatory, threatening or bullying in nature staff must not respond and should report the communication to the Headteacher, IT Network Manager or DSL.
- 7.6. Staff personal email addresses, text messages or social media must not be used for communicating with parents regarding matters involving any kind of school business.
- 7.7. Staff should not be seen using social media or any personal emails whilst teaching or around pupils.
- 7.8. For quality control and monitoring purposes, whole class/group emails for parents should be sent out via the office rather than by individual members of staff.
- 7.9. Staff email addresses are not published on the school website. Only official email addresses should be used to identify members of staff. Staff personal information should not be posted and made available online.
- 7.10. Pupils should use their Google Classroom accounts to upload homework and communicate with their classroom teacher. However, under certain circumstances, pupils may email homework to a member of staff who has set it using ONLY that individual staff member's school email address (e.g. teachername@oakwoodschool.co.uk) and no correspondence should be entered into.
- 7.11. Unfortunately, the school cannot control internet access via non-school provided means such as mobile networks and therefore it is feasible for individuals to access any content via 3G, 4G and 5G access. The school protects its pupils by restricting access to mobile phones on site and encourages staff to be responsible in their usage.

Pupils

- 7.12. All pupils are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work including assignments, research and projects. Pupils should be aware that email communications through the school network and school email addresses are monitored.
- 7.13. The school will ensure that there is appropriate and strong IT monitoring and virus software. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work or research purposes, pupils should contact the IT Manager or IT team for assistance.
- 7.14. Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to their class teacher, a member of staff, IT Network Manager or DSL.
- 7.15. Pupils are made aware of the expectations regarding safe internet and computer usage through agreements signed by parents/carers (and pupils in the Prep School).
- 7.16. Pupils should be aware that all internet usage in school and remotely via the school's Google Mail system and its Wi-Fi network is monitored.

8. Use of social media

Staff

- 8.1. Staff must not access social networking sites, personal email or any website or personal email which is unconnected with school work or business from school devices or whilst teaching or in front of pupils. Such access may only be made from staff members' own devices whilst in the staff room or staff-only areas of school.
- 8.2. When accessed from staff members' own devices or off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school in accordance with the Staff Code of Conduct.
- 8.3. The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; Apps; video/photo sharing sites; chat rooms and messaging platforms. All members of the school community are expected to engage with social media in a positive, safe and responsible manner.
- 8.4. Any online communications, whether by email, social media, private messaging or other, must not:
 - place a child or young person at risk of, or cause, harm
 - bring Oakwood School into disrepute
 - breach confidentiality
 - breach copyright
 - breach data protection legislation
 - do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
 - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age
 - using social media to bully another individual
 - posting links to or endorsing material which is discriminatory or offensive
 - otherwise breach the Staff Code of Conduct or Child Protection and Safeguarding Policy
- 8.5. Under no circumstances should school pupils or parents be added as social network 'friends' or contacted through social media. Staff should not initiate friend requests nor follow pupils via social media.
- 8.6. Reference to any pupils, staff or parents should not be made using social media channels. Staff are reminded they should use social networking sites with extreme caution, being aware of the nature of what is published online and its potential to impact on their professional position. This is reinforced during staff induction training and at regular meetings or safeguarding training events.

Pupils

- 8.7. The school expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to an individual or others. The school takes misuse of technology by pupils very seriously and incidents will be dealt with

under the Behaviour Management, Rewards & Sanctions Policy, Safeguarding and Child Protection Policy and Anti-Bullying Policy as appropriate.

- 8.8. Given the age of pupils at Oakwood School (ages 2-11), pupils are not expected to use social media platforms, as most have age restrictions of 13+. However, online safety education includes discussion about social media to prepare pupils for safe use in the future and to address any exposure they may have at home.

9. Data Protection

- 9.1. Please refer to the Data Protection Policy and the IT Acceptable Use Policy for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the school.
- 9.2. Staff and pupils are expected to save all data relating to their work to their school laptop/PC or to the school's Google Drive Account as per the IT Acceptable Use Policy.
- 9.3. Each member of staff has a personal folder on the server in which they can store their work. This can be accessed by any computer linked to the network. However, staff are encouraged to save all data relating to their work to their Google Drive. Pupils are expected to save all their data relating to their work to their Google Drive and personal account.
- 9.4. Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending. The school discourages removable media to be used to store school data.
- 9.5. Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by the school.
- 9.6. Memory sticks are not permitted to be used within school computers unless virus checked by the IT Network Manager on a standalone PC.
- 9.7. Staff should also be particularly vigilant about scam/phishing emails (and similar) which could seriously compromise the school's IT security and/or put at risk sensitive personal data (and other information) held by the school. If in any doubt, do not open a suspicious email or attachment and notify the IT Manager or IT team in accordance with the Data Protection Policy and IT Acceptable Use Policy.
- 9.8. Staff should not open hyperlinks in emails or as attachments in emails, unless the source is known and trusted. If they are unsure of any attachment, they should contact the IT Network Manager to ensure the document is safe.
- 9.9. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Network Manager, Head of Digital Development or DSL.

10. Password Security

- 10.1. The Pupils and staff have individual school network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.
- 10.2. All members of staff should:
- use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers), which should be changed every 6 months
 - not write passwords down
 - not share passwords with other pupils or staff
- All pupils should:
- use the passwords provided by the school
 - not share passwords with other pupils or staff
- 10.3. Passwords protect the school's network and computer system and are an individual's personal responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as widely-used personal passwords. Staff, Visitors and Volunteers should not let anyone else know their password, nor should they keep a list of passwords where they may be accessed. If compromised, staff must change their password immediately. Staff, Visitors and Volunteers should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which they do not have access rights.
- 10.4. Oakwood School's password policy for system/network access is that the password must have a minimum of 8 characters and include at least one of the following: upper case letter, lower case letter, number and a symbol. The school may require that system/network passwords are periodically changed.
- 10.5. Oakwood School's password policy for e-mail accounts is as for system/network access, however this is more stringent than required by Google Mail (a minimum of 8 characters). E-mail passwords must not be the same as any other passwords used by the user. 2-step authentication is not required for staff email passwords at present, but may be introduced in the future if there are concerns about the security of email account passwords. The school may require that e-mail account passwords are periodically changed and they must be changed immediately should there ever be a concern regarding a possible security breach.
- 10.6. To enhance the security of staff email accounts and protect sensitive school data, Oakwood School has implemented Multi-Factor Authentication (MFA) for all Google Workspace accounts. MFA adds an additional layer of security beyond just a password, significantly reducing the risk of unauthorized access even if a password is compromised.
- 10.7. Multi-Factor Authentication requires users to provide two or more verification factors to access their account. In addition to entering their password, staff must verify their identity using a second method, such as:
- A verification code sent to a registered mobile device via SMS
 - A prompt through the Google Authenticator app or similar authentication app
 - A security key (hardware token)
 - A backup code (for emergency access)

- 10.8. All staff members are required to:
- Enroll in MFA for their Google Workspace account within 7 days of this policy taking effect or upon joining the school
 - Register at least one primary authentication method (preferably a mobile authenticator app) and one backup method
 - Keep their registered devices and contact information up to date
 - Store backup codes in a secure location (not on the device used for primary authentication)
 - Never share authentication codes or bypass MFA security measures
- 10.9. All staff members will receive instructions and support from the IT Network Manager or IT team to set up MFA on their Google Workspace accounts.
- 10.10. Once MFA is enabled, staff will be prompted for a second form of verification when:
- Signing in from a new device
 - Signing in after a period of inactivity
 - Accessing particularly sensitive information or settings
 - The system detects unusual activity or a security risk
- 10.11. If staff members experience issues with MFA, such as:
- Lost or broken authentication device
 - Not receiving verification codes
 - Locked out of their account
- They should immediately contact the IT Network Manager or IT team for assistance. The IT department maintains secure processes for account recovery that verify the staff member's identity before restoring access.
- 10.12. There are security considerations for staff:
- Staff should never respond to unsolicited requests for their authentication codes, even if the request appears to come from the school or IT department
 - Authentication apps (such as Google Authenticator, Microsoft Authenticator, or Authy) are preferred over SMS for security reasons, as they are less vulnerable to interception
 - Staff should report any suspicious login attempts or notifications about unrecognized devices accessing their account to the IT Network Manager and DSL immediately
 - Backup codes should be treated with the same level of security as passwords and stored separately from the device used for primary authentication
- 10.13. The requirement for MFA may only be waived in exceptional circumstances with written approval from both the Headteacher and the DSL, and such exceptions will be reviewed regularly.
- 10.14. For younger pupils, staff will help them create and remember appropriate passwords. Pupils are taught about password security as part of their computing and online safety education.
- 10.15. Staff, Visitors and Volunteers should:
- not disclose their username or password to anyone else, nor try to use any other person's username and password

- understand that they should not write down or store a password where it is possible someone may have access to steal it.

11. Safe Use of digital and video images or recordings

- 11.1. 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, stalking or grooming 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.
- 11.2. 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 (personal) images on the internet (e.g. on social networking sites) and follow the school's policy on official social media posting.
- 11.3. The publication of digital images on the internet or through social media channels carries an inherent risk that they could be used in an inappropriate way by individuals looking to cause harm or embarrassment to them. Care must be taken when using photographs or video footage of pupils on the school website and social media channels. Digital images and the footprint they receive may stay on the internet indefinitely.
- 11.4. A range of school cameras, Chromebooks, iPads and recording equipment is available for staff and volunteers to use to support educational aims. All photographic images of pupils should be taken and stored on school equipment, not on personal devices. If personal specialised equipment is being used for a particular function or reason, it should be authorised by the IT Network Manager, DSL and Headteacher with a clear understanding that any digital media will be transferred to the school network and not stored on personal devices at home or in school. Further information can be found in the following policies:
 - Mobile Devices (including Mobile Cameras) Policy for Staff, Governors, Volunteers and Visitors
 - Taking, Storing and Using Images of Children Policy
 - IT Acceptable Use Policy
- 11.5. As part of their PSHE and ICT curriculum, pupils are taught about how images can be abused by individuals looking to cause harm or embarrassment. Children are educated in the risks of taking, using, sharing, publishing, distributing and storing their own personal images. Pupils are advised not to place personal images on any social networking space and are given guidance to review the background of their images which may give information to identify themselves or their location.
- 11.6. When using digital images in a public digital forum, the school ensures that pupils are not referred to by name on the image or video and any full names of pupils are not given in the titles or film credits.
- 11.7. When using digital/video images, the school takes care to ensure that images contain individuals who are appropriately dressed and are not undertaking activities that may bring the pupil or the school into disrepute.

- 11.8. On enrolling with the school, parents/carers are required to give their permission regarding the taking and publishing of photos, video footage or images on the school website or social media channels.
- 11.9. The uploading of images to the school website and social media pages is restricted to the school's Marketing Manager. Images selected for publication comply with good practice and follow guidance as set out in the Taking, Storing and Using Images of Children Policy.
- 11.10. Parents/carers and pupils are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by GDPR). To respect everyone's privacy and in some cases an individual's personal protection, images should not be taken, used, shared, published or distributed of other children without the expressed permission (or parental/carers permission) of the identifiable individuals contained within. Videos and digital images are permitted for personal use only.
- 11.11. All online lessons are conducted using Google Meeting. Lessons should be recorded and stored within the appropriate folder for safeguarding reasons. Refer to the Remote Education Policy within the Teaching and Learning Policy for further details.
- 11.12. Alongside our Staff Behaviour Code of Conduct policy, colleagues and pupils should ensure:
 - they and other family members on screen are appropriately dressed
 - teaching takes place from an appropriate space
 - nothing inappropriate is seen or heard in the background. The 'blur' background function may be useful in these circumstances
 - the language used by staff and pupils in the online meeting is appropriate for all persons who may be able to hear the conversation
 - 1:1 conversations with parents or pupils using remote online software should be made through Google Meeting or Zoom. Conversations should be recorded for safeguarding reasons and participants made aware of this at the start of the meeting

12. Artificial Intelligence

- 12.1. Given the age of pupils at Oakwood School (ages 2-11), the school does not permit pupils to use generative AI tools such as ChatGPT on school devices or systems. Most generative AI platforms have minimum age requirements of 13+ which our pupils do not meet.
- 12.2. Staff may only use AI tools with prior approval from the Headteacher and DSL, and must never input any personal or confidential information about pupils or families into such tools.
- 12.3. Personal or confidential information should not be entered into generative AI tools. This technology can potentially store and/or learn from data inputted and users should consider that any information entered into such tools may be released to the internet.
- 12.4. Note: Paid-for versions of AI tools or AI tools licensed for use within the school's broader software ecosystem may offer assurances that input data will not be used externally or for training the tool. However, the school approaches such assurances with caution and ensures clarity on exactly how any input data will be used/retained.
- 12.5. It is also important to be aware that the technology, despite its advances, still produces regular errors and misunderstandings and should not be relied on for accuracy. In particular, pupils should not use these tools to answer questions about health/medical/wellbeing issues,

or indeed anything of a personal nature. It is always best to seek help and recommendations as to reliable resources from a member of staff or the DSL.

- 12.6. Oakwood School will evaluate the benefits and risks of any proposed use of generative AI by staff or pupils, with particular regard to risk associated with safeguarding, data protection and the possibility of bias and discrimination. Any approved use of AI will be kept under review and the school will remain alert to the possibility of unauthorised use.
- 12.7. Pupils will be taught age-appropriate information about AI as part of their computing and online safety curriculum to prepare them for safe and responsible use in the future.

13. Security and Management of Information Systems

- 13.1. The school takes all reasonable, practical and precautionary steps to ensure that the infrastructure/network is secure and safe for our staff and pupils including:
 - implementing and regularly updating anti-virus and anti-spam systems on our email system. Any virus activities or suspicions must be reported to the IT Network Manager immediately
 - the appropriate use of user logins, passwords and best security practices to access our network and the school gives guidance on the reasons for always logging off and for keeping all passwords secure
 - specific user logins and passwords enforced for all school users
 - the school provides enhanced/differentiated user-level filtering; however, internet access is filtered for all users. Illegal content is filtered by the filtering provider (Smoothwall) by actively employing the Internet Watch Foundation CAIC list
 - Smoothwall restricts and monitors content access by both pupils and staff. Pupils and staff are safe from inappropriate and/or terrorist and extremist material when accessing the internet in school
 - the IT Network Manager regularly reviews the effectiveness of the filtering system as well as monitoring and recording the activity of all users on the school technical systems. Any actual/potential incidents or security breaches are immediately reported to the IT Network Manager or DSL
 - the IT Network Manager may view a computer screen at any time without the user's knowledge to ensure the system is being used appropriately
 - appropriate security measures are in place to protect servers, firewalls, routers, wireless systems, work stations and mobile devices which might threaten the security of the school systems and data
 - provision of temporary access to 'guest users' is on a case by case basis and the extent of their access is limited
 - all staff and pupils have access to their own Google Drive account, which is accessed using their school email address. Pupil accounts are restricted so that the mail function is not accessible for younger children
 - not using portable media without specific permission from the IT Network Manager and any member of staff or pupil wishing to connect a portable device to the school's network is asked to arrange in advance with the IT department to ensure that viruses are not introduced to the system

- devices connecting to the school's Wi-Fi systems are required to enter a password to ensure no unsupervised access is obtained by pupils using various portable devices
- an inventory of all school hardware and software is maintained by the IT Network Manager

14. Breach Reporting

- 14.1. The law requires the school to notify personal data breaches to the Information Commissioner's Office (ICO) and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- 14.2. This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:
- loss of an unencrypted laptop, USB stick or a physical file containing personal data
 - any external hacking of the school's systems, e.g. through the use of malware
 - application of the wrong privacy settings to online systems
 - misdirected post, fax or email
 - failing to bcc recipients of a mass email
 - unsecure disposal
- 14.3. The school will generally report personal data breaches to the Information Commissioner's Office (ICO) without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school will keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If either staff or pupils become aware of a suspected breach, the Headteacher or Bursar, and IT Manager, will be informed immediately.
- 14.4. Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

15. Misuse

- 15.1. Oakwood School will not tolerate illegal activities or activities that are in breach of the policies referred to above. Where appropriate the school will report illegal activity to the police and/or the local safeguarding partnerships. If a member of staff discovers that a child or young person is at risk as a consequence of online activity they should report it to the DSL. The DSL then may seek assistance from the CEOP, the LADO, and/or its professional advisers as appropriate.

- 15.2. The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Safeguarding and Child Protection and Behaviour Management, Rewards & Sanctions Policies.
- 15.3. All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or worrying issues to a member of the pastoral staff.
- 15.4. Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures (in particular the Safeguarding and Child Protection Policies).
- 15.5. The school adopts a zero-tolerance approach to any cyber bullying incidents and any abusive behaviour which is notified to staff between pupils will be reported to the DSL immediately. For further information on dealing with child-on-child abuse, see the Safeguarding and Child Protection Policy.
- 15.6. For further guidance on what to do if there is an online safety concern, review the online safety process incident flowchart in Appendix A.

16. Complaints

- 16.1. Oakwood relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the form teacher in the first instance, who will undertake an immediate investigation and liaise with the Senior Leadership Team plus any additional members of staff or pupils who are involved. For more serious concerns, complaints should be addressed to the Online Safety Coordinator who will liaise with the senior leadership team and undertake an investigation where appropriate. Please see the Complaints Policy for further information.
- 16.2. Incidents of, or concerns around online safety will be recorded in accordance with the Safeguarding and Child Protection policy and reported to the school's Online Safety Coordinator and the DSL in accordance with the school's Safeguarding and Child Protection Policy.
- 16.3. If you become aware of a breach of this policy or concerns around online safety, or you are concerned that a member of the school community is being harassed or harmed online you must report it to the Headteacher or a member of the Senior Leadership Team. Reports will be treated in confidence.

17. Compliance with related school policies

- 17.1. Staff will ensure that they comply with this Online Safety Policy and other relevant policies, including:
 - Retention of Records Policy
 - Safeguarding and Child Protection Policy (including KCSIE 2025)
 - Anti-Bullying Policy
 - Data Protection Policy
 - Mobile Devices (including Mobile Cameras) Policy for Staff, Governors, Volunteers and Visitors
 - Taking, Storing and Using Images of Children Policy

- Staff Code of Conduct
- Behaviour Management, Rewards & Sanctions Policy
- PSHE and Well-being Policies

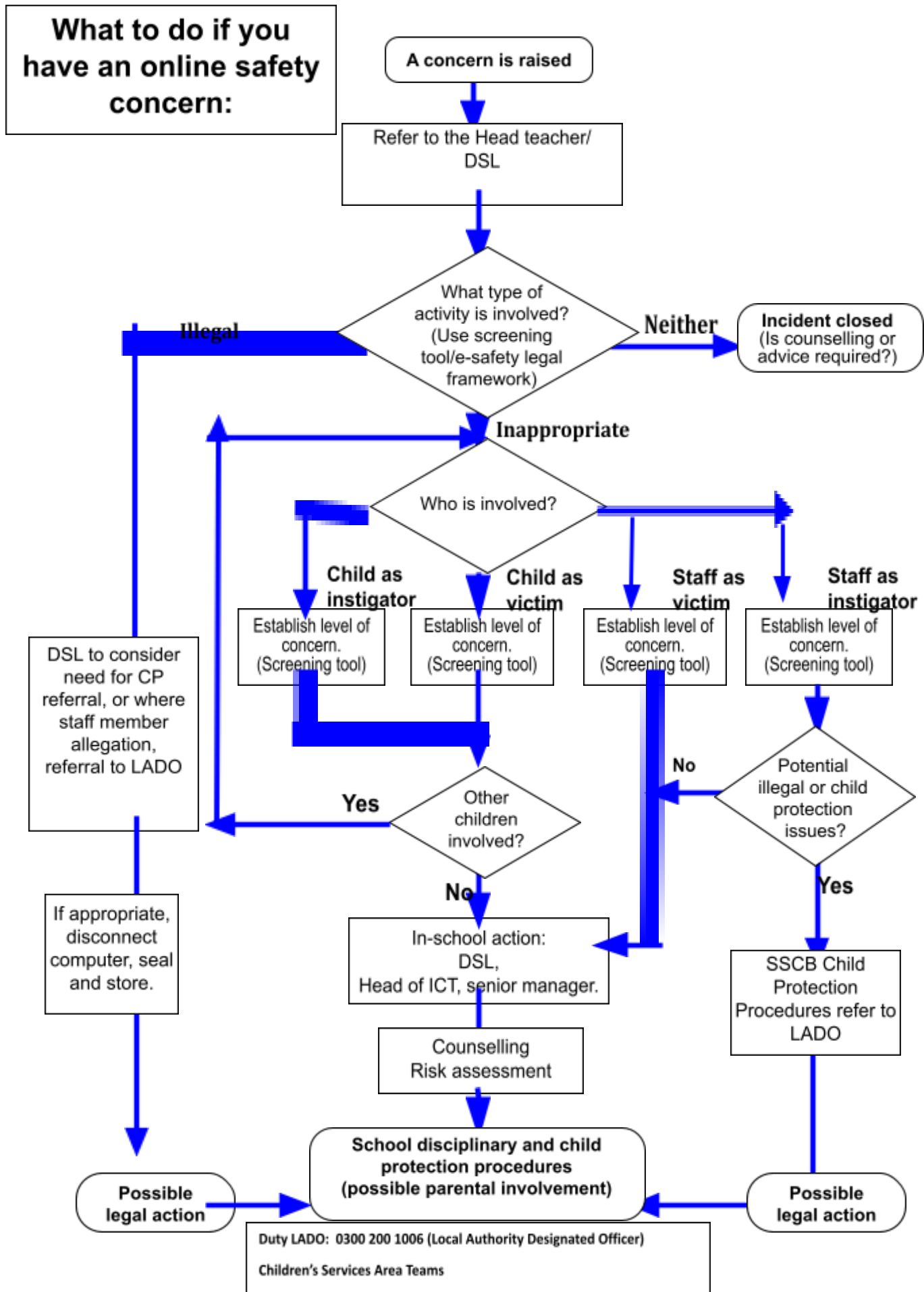
18. Retention of Digital Data

- 18.1. Staff and pupils must be aware that all emails sent or received on school systems will be kept in archive whether or not deleted and email accounts will be closed immediately upon leaving the school.
- 18.2. Important information that is necessary to be kept should be held on the relevant personnel or pupil file, not kept in personal folders, archives or inboxes. Hence it is the responsibility of each account user to ensure that important information (or indeed any personal information that they wish to keep, in line with school policy on personal use) is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's email deletion protocol.
- 18.3. If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact the Operations Manager or IT Manager.

19. Use of Property

- 19.1. Any property belonging to the school should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the IT Manager.

Appendix A: Online Safety Process Incident Flowchart



APPENDIX B:



IT Acceptable Use Policy – Staff, Visitors & Volunteers

Implementation Date: October 2018
Date / Term of last review: Michaelmas Term 2025

This policy applies to the whole school including those in the EYFS.

Author:	Lucy Strong, Operations Manager
Approval:	Clare Bradbury, Headteacher
Next Review Date:	Michaelmas Term 2026

For office use only:

Website	Required	✓
Internal Staff purposes only		

1. **Aims and objectives**

- 1.1. Technology plays an enormously important part in the lives of all society including children and young people. To this end, technology has transformed the entire process of teaching and learning at Oakwood School. It is a crucial component of every academic subject, and is also taught as a subject in its own right. All of our classrooms are equipped with electronic whiteboards, projectors and computers.
- 1.2. This policy applies to all members of the school community, including staff, pupils, parents, contractors and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers (but access to systems is not intended in any way to imply an employment relationship). 'Parents' include, where applicable, pupils' carers and those with parental responsibility. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.
- 1.3. The IT Acceptable User Policy is intended to ensure:
 - That staff, visitors and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
 - The school ICT 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 ICT in their everyday work. The school will try to ensure that staff, visitors and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupil learning and will, in return, expect staff, visitors and volunteers to agree to be responsible users.

2. **Online behaviour**

- 2.1. As a member of the school community you agree to the following principles in all of your online activities:
 - I have an awareness of all safeguarding systems and policies in place at Oakwood to safeguard children effectively (reference KCSIE 2025).
 - I ensure that my online communications, and any content shared online, are respectful of others and composed in a way I would wish to stand by.
 - I will not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, harassment or extremism, or raises safeguarding issues).
 - I will not upload, download or access any material which are illegal (including but not limited to: child sexual abuse images, racist or pornographic) and inappropriate and may cause harm or distress to others.
 - I respect the privacy of others. I will not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission and in writing.
 - I will not use my personal equipment to record these images, unless I have permission to do so. I will abide by the guidelines as laid out by the Mobile Devices (including Mobile Cameras) Policy for Staff, Governors, Volunteers and Visitors.
 - I will not access or share material that infringes copyright, and shall not claim the work of others as my own.
 - I will not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.

- I shall not use their personal email, or social media accounts to contact pupils or parents, and pupils. Parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.
- I will only use chat and social networking websites in accordance with the school policy.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

3. **When using the school's IT systems**

3.1. The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff should keep their personal, family and social lives separate from their school IT use and limit, as far as possible, any personal use of these accounts. Again, please be aware of the school's right to monitor and access web history and email use.

3.2. Whenever using the school's IT systems (including by connecting personal device(s) to the network) staff, visitors and volunteers should follow these principles:

- I will only access school IT systems using my own username and password. I will not share my username or password with anyone else.
- I will not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and will not attempt to access parts of the system that I do not have permission to access.
- I will not attempt to install software on, or otherwise alter, school IT systems.
- I will not use the school's IT systems in a way that breaches the principles of online behaviour set out above and within the Oakwood E-safety policy.
- I will remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.
- I will only communicate with parents/carers using official school systems.
- All communications I engage in will be professional in tone and manner. I recognise and appreciate that there may be different opinions on various issues and will ensure that I do not use aggressive or inappropriate language.
- I will not open hyperlinks in emails or as attachments in emails, unless the source is known and trusted. If I am unsure of any attachment, I will contact the IT Network Manager to ensure the document is safe.

4. **Passwords**

4.1. Passwords protect the School's network and computer system and are an individual's personal responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as widely-used personal passwords. Staff, Visitors & Volunteers should not let anyone else know their password, nor should they keep a list of passwords where they may be accessed. If compromised, staff must change their password immediately. Staff, Visitors & Volunteers should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which they do not have access rights.

4.2. Oakwood School's password policy for system / network access is that the password must have a minimum of 8 characters and include at least one of the following: upper case letter, lower case letter, number and a symbol. The School may require that system / network passwords are periodically changed.

4.3. Oakwood School's password policy for e-mail accounts is as for system / network access, however this is more stringent than required by Google Mail (a minimum of 8 characters). E-mail passwords must not be the same as any other passwords used by the user. 2-step authentication is not required for staff email passwords at present, but may be introduced in the future if there are concerns about the security of email account passwords. The School may require that e-mail account passwords are periodically changed and they must be changed immediately should there ever be a concern regarding a possible security breach.

4.4. When considering password security:

- 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 someone may have access to steal it.

5. **Use of Property**

5.1. Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the IT Manager.

6. **Use of personal devices or accounts and working remotely**

6.1. All official school business must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Similarly, personal business should not be conducted on school systems and using school email accounts. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, or cloud – must be done in accordance with school policies regarding data security, IT acceptable use, confidentiality, etc. USB memory sticks are not permitted to be used.

6.2. Personal devices must be subject to appropriate safeguards in line with the school's policies, for example, the Mobile Devices (including Mobile Cameras) Policy for Staff, Governors, Volunteers and Visitors.

6.3. When using the internet or personal devices in my professional capacity or for school sanctioned personal use I agree:

- To ensure that I have permissions to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music or videos)
- When using my own mobile device in school, I will follow the rules and arrangements as set out in this agreement as if I were using a school related device.

7. **Monitoring and access**

7.1. Staff, parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others. The school has an internet content filter in place to protect and safeguard pupils, staff and others.

7.2. Any personal devices used by pupils, whether or not such use is permitted, may be confiscated and examined under such circumstances. The school may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy

8. **Compliance with related school policies**

8.1. Staff will ensure that they comply with the school's E-Safety Policy and other relevant policies, e.g. Retention of Records, Safeguarding, Anti-Bullying, Data Protection.

9. **Retention of digital data**

9.1. Staff and pupils must be aware that all emails sent or received on school systems will be kept in archive whether or not deleted and email accounts will be closed immediately upon leaving the school.

9.2. Important information that is necessary to be kept should be held on the relevant personnel or pupil file, not kept in personal folders, archives or inboxes. Hence it is the responsibility of each account user to ensure that important information (or indeed any personal information that they wish to keep, in line with school policy on personal use) is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's email deletion protocol.

9.3. If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact the Operations Manager or IT Manager.

10. **Breach reporting**

10.1. The law requires the school to notify personal data breaches, to the Information Commissioner's Office (ICO) and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

10.2. This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, e.g. through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

10.3. The school will generally report personal data breaches to the Information Commissioner's Office (ICO) without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school will keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If either staff or pupils become aware of a suspected breach, the Headteacher or Bursar, and IT Manager, will be informed immediately.

10.4. Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

11. **Breaches of this policy**

11.1. A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. In addition, a deliberate breach may result in the school restricting your access to school IT systems.

11.2. If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you must report it to the Headteacher or a member of the Senior Leadership Team. Reports will be treated in confidence.

11.3. Staff, Visitors and Volunteers are responsible for their actions in and out of school. In following the guidance provided by this policy:

- I understand that this agreement 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 off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand and should I fail to comply with this Agreement, I could be subject to disciplinary action.



**IT ACCEPTABLE USE POLICY AGREEMENT FOR STAFF,
VISITORS AND VOLUNTEERS**

I confirm that I have read, understood and accept the contents of the IT Acceptable Use Policy.

I agree to abide by its contents when using school ICT systems and my own devices on the school network.

Name: (PLEASE PRINT)

Signature:

Date:



IT ACCEPTABLE USE POLICY AGREEMENT FOR PREP SCHOOL PUPILS

Oakwood endeavours to ensure that you have reliable access to digital technologies to enhance your learning and will, in return, expect you to agree to be responsible users. This IT Acceptable Use Policy is intended to ensure:

- That pupils of Oakwood School are responsible users and stay safe while using the internet and other digital technologies.
- That Oakwood School IT systems and other users are protected from accidental or deliberate misuse that could put the security of the systems and other pupils at risk.

In using technology responsibly:

- 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 understand that Oakwood ICT systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have been given permission to do so.
- I understand that to keep me safe, Oakwood School will monitor my use of the systems, devices, and digital communications.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I understand that I am responsible for my actions, both in and out of school.
- I understand that Oakwood 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 Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

For my own personal safety:

- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will not arrange to meet people off-line that I have communicated with on-line.

- I will immediately report to a trusted adult any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

Personal Conduct

- I will act as I expect others to act toward me
- I will not use Oakwood systems or devices for on-line gaming or video broadcasting.
- I will respect other pupils' work and property and will not access, copy, remove or otherwise alter any other user's files, without their knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive, or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I will not bring my own personal devices (mobile phones / apple watches / tablets / laptops etc) into school unless I have been given direct permission to do so.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

If you do not sign this agreement, you may not be granted access to school ICT systems.

I have read and understand the above and agree to follow these guidelines:

Pupil's Name: _____

Signature: _____

Date: _____

Parent Name: _____

Counter Signature: _____

Date: _____



IT ACCEPTABLE USE POLICY AGREEMENT FOR PRE-PREP SCHOOL PUPILS

Using the computer and internet safely

In an increasingly digital world, we actively encourage our pupils to use computers and the internet safely. In order to assist with this, we would be grateful if you would go through the points below with your child and sign when you feel they have understood.

This is how we will stay safe when we use computers:

- I will only go online when an adult is with me.
- I will only use my own username and password to log on
- I will only use apps and programs with an adult's permission.
- I will only click on links and buttons when I know what they do.
- I will keep information about me safe online.
- I will always be kind online.
- I will always tell an adult if something online makes me feel upset, unhappy, or worried.
- I know that if I break the rules I might not be allowed to use a computer.

Pupil's Name: -----

Parent's Signature: -----

Date: -----

APPENDIX C:



**BRING YOUR OWN DEVICE:
OAKWOOD PERMISSION FORM - PUPILS**

Name of Pupil:	
-----------------------	--

This Consent Form is valid for:

The duration of your time at the School	Yes/No (<i>please indicate</i>)
Some shorter time – please specify	

Parents of pupils who wish to use or connect a personally owned electronic device to the school network within Oakwood School, must read and sign this agreement and return it to the Designated Safeguarding Lead and/or Headteacher.

1. The pupil is responsible for their own device and ensures its safe storage and use at all times. The school is not responsible for the security of the device.
2. The pupil is responsible for the proper care of the personal device, including its maintenance, repair, replacement or any modifications needed to use the device at school.
3. The school reserves the right to inspect a pupil's personal device if there is reason to believe that he/she has violated school policies, procedures, school rules or has engaged in other misconduct while using the personal device.
4. The pupil must comply with a teacher request to shut down the computer or close the screen.
5. The pupil may not use the devices to record, transmit or post photos or video of a person or persons on the school site. Nor can any images or video recorded at school be transmitted or posted at any time without the express permission of the Teacher or Headteacher.
6. The pupil's device will have legal versions of the operating system, software and Apps. The school will not connect a device to the school network unless these are in place.
7. The activity of each device will be logged if it is connected to the school's internet site. The violation of any school policies, procedures or school rules involving a pupil's personally owned device may result in the withdrawal of permission to use the device in school and/or disciplinary action.
8. The pupil's device must not have access to 3G, 4G or 5G networks whilst on school property. SIM cards should be removed at all times.
9. The school accepts no liability for any loss or damage to pupil's personal devices brought on to school property.

I have read and understood the policy and guidelines relating to my child bringing their own devices to school and have discussed these with my child/ren appropriately to ensure they understand the agreement in place.

I understand that any violation of the above may result in the loss of device privileges as well as additional disciplinary action for my child.

Signature of Parent Date

Print Name