OAK GREEN SCHOOL
Believe, Achieve, Succeed

Non-Statutory

Online Safety including Filtering and Monitoring and Cyber Security

Contents

1. Introduction and overview
   - Rationale and scope
   - Roles and responsibilities
   - How the policy can be communicated to staff/pupils/community
   - Handling complaints
   - Review and monitoring

2. Education and curriculum
   - Pupil Online Safety curriculum
   - Staff and governor training
   - Parent awareness and training
   -
3. Expected conduct and incident management
   - Expected Conduct
   - Staff / Pupil use of personal devices
   - Incident Management
   - Cyberbullying

4. Managing the COMPUTING infrastructure
   - Internet access, security (virus protection) and filtering
   - Network management (user access, backup, curriculum and admin)
   - Password policy
   - E-mail
   - School website
   - Social networking
   - Data security
   - Management information system access
   - Data transfer

5. Data Security: Management Information System Access and Data Transfer
   - Strategic and operational practices
   - Technical solutions

6. Asset disposal

1. Introduction and Overview

Online Safety encompasses internet technologies and electronic communications such as mobile phones and smart devices as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

All adults who come into contact with children and young people in their work have a duty of care to safeguard and promote their welfare. (1989 Children Act and Child Care Act 2000).

The Online Safety Act (2023) sets out the following for protecting children:-

> ***"Platforms likely to be accessed by children will need to:***
>
> - ***prevent access to material that is harmful for children, such as pornography.***
> - ***ensure there are strong protections from activity which is harmful to children, which we expect will include harms such as bullying.***
>
> ***If a child does encounter harmful content or activity, parents and children will be able to report it easily. Platforms will be required to take appropriate action in response.***
>
> ***Platforms will also have a duty to report any child sexual exploitation and abuse content that they encounter to the National Crime Agency, to assist with law enforcement efforts to stamp out this appalling crime."***

The Online Safety Act (2026) has been updated to require digital platforms to scan private messages and user content before delivery using automated systems. This means platforms must detect and block harmful content before it reaches recipients, including private messages (using AI-powered scanning). The change stems from the Online Safety Act 2023. The two new 'priority offences' that will trigger this action are:

- Cyberflashing
- Encouraging or assisting serious self-harm

All school staff are required to familiarise themselves with Keeping Children Safe in Education 2025 Statutory Guidance for schools and colleges Part One which can be accessed via the following link:

https://assets.publishing.service.gov.uk/media/6a47c29b1c8bd7ce25a5eb6d/Keeping_children_safe_in_education_2026__part_one.pdf

The Keeping Children Safe in Education (KCSIE) Statutory Guidance for Schools and Colleges was updated on 1st September 2026 and places a heavier emphasis on emerging digital risks, artificial intelligence, and leadership accountability.

KCSiE 2026 has been updated to reflect the rapid growth of artificial intelligence the safe and effective use of generative AI in education. All incidents involving the sharing of indecent or semi-indecent images (whether "digitally altered or wholly generated using artificial intelligence) now require a safeguarding response, whether they are consensual or non-consensual.

For the scope of online safety requirements please refer to the complete document here:

https://assets.publishing.service.gov.uk/media/6a4cf903b7203c4c023fd2f3/Keeping_children_safe_in_education_2026_.pdf

KCSiE 2026 also includes the following references to Information security and access management:

"Governing bodies and proprietors should take measures to safeguard children by protecting personal information and ensuring their school or college has appropriate cyber security systems in place. This should be approached as part of the school or college's wider safeguarding responsibilities. As part of this, schools and colleges should consider implementing measures in line with the Cyber security standards for schools and colleges. The Cyber security standards for schools and colleges outline actions that schools and colleges should consider implementing to strengthen resilience, reduce the risk of disruption, prevent data breaches, and mitigate safeguarding risks."

This policy also includes references to Cybercrime.

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include:

• unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded

• 'Denial of Service' (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources, and,

• making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skills and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low-level cyber-dependent offences and divert them to a more positive use of their skills and interests. Note that Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety

The following policy will apply to all members of Oak Green School Community (including staff, students/pupils, Governors, volunteers, parents/carers, visitors and community users) who have access to its 'Computing Systems', both on and off the premises.

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

Oak Green School will deal with any such incidents 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 takes place out of school.

The school's Online Safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Artificial Intelligence for machine learning, Social Media and Networking, Mobile Phones, Personal Devices & Imaging and Data Protection Policies.

Rationale

The purpose of this policy is to:

- Outline the expectations for all members of the school community at Oak Green School with respect to the use of computing-based technologies.
- Safeguard and protect the staff and children of Oak Green School and comply with GDPR (General Data Protection Regulation)
- Enable staff and children to work with the internet and other communication technologies safely and to monitor their own standards and practice.
- To provide clear expectations of behaviour and/or codes of practice relevant to the responsible use of the internet for educational, personal and recreational use.
- To clearly structure how to deal with online abuse such as cyberbullying.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To minimise the risk of misplaced or malicious allegations made against adults who work with children.

The main areas of risk for our school community can be summarised as follows:

Content

- Ignoring age ratings while playing online games (exposure to violence associated with often racist/foul language, addiction, in -app purchases)
- Exposure to inappropriate content.
- Ignoring age restrictions on social networking websites such as Instagram, Facebook, YouTube, Snapchat, WhatsApp, etc…
- Data breaches
- Hate sites, sites inciting radicalisation and/or extremism

- Content validation: how to check authenticity and accuracy of online content.

Contact

- Grooming
- Sexting
- Trolling
- Cyberbullying in all forms
- Identity theft and sharing passwords

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and wellbeing (amount of time spent online)
- Copyright
- Inappropriate Messaging

Commerce

- Phishing
- Inappropriate advertising
- Spoofing
- Access to online gambling sites

Roles and Responsibilities

The following section outlines the Online Safety roles and responsibilities of individuals and groups within Oak Green School.

Governors:

The role of the Governors responsible for Data Protection/Filtering and Monitoring and Safeguarding will include:

- Regular meetings with the Computing Lead, Online Safety Lead and Data Protection Officer.
- Reporting back at Governor meetings
- Ensuring that the school follows the current Online Safety advice to keep the children and staff safe.
- The regular monitoring of any Online Safety incident logs (see GDPR log).
- The regular monitoring of filtering
- To approve the Online Safety Policy and review the effectiveness of the policy.
- To support the school in encouraging parents and the wider community to become engaged in Online Safety activities.

Co-Headteachers:

- To take overall responsibility for Online Safety provision
- To take overall responsibility for data and data security being GDPR compliant
- To ensure that the school uses an approved, filtered Internet Service, which complies with current statutory requirements.
- The Co-Headteachers and at least another member of the SLT should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.

- The Co-Headteachers are responsible for ensuring that the Data Protection Officer, Computing Lead and Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues.
- To receive regular monitoring reports about Online Safety from the Online Safety Lead.
- The Co-Headteachers will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role.

Designated Safeguarding Leads

- Designated Safeguarding Leads to understand the school's filtering and monitoring systems and processes.
- To receive regular monitoring reports about filtering and monitoring.
- To be aware of any trends with regards to online safety.
- To be aware of any alerts created by the school's monitoring software.

Online Safety Lead:

An Online Safety Lead is appointed to:

- Promote an online safety culture under the direction of the senior leadership team.
- Act as a key point of contact on all Online Safety issues.
- Raise awareness and understanding of Online Safety to all stakeholders, including parents and carers.
- In conjunction with the Computing Lead embed Online Safety in staff training, continuing professional development and across the curriculum.
- Take day to day responsibility for Online Safety issues.
- Review the school Online Safety Policy regularly and in accordance with new legislation.
- Ensure all staff are aware of the procedures that need to be followed in the event of an Online Safety breach.
- Providing training and advice for staff.
- Receive reports of Online Safety incidents and report directly to the Data Protection Officer (see GDPR Log).
- Report regularly to the SLT and/or Governors.

Technical Staff:

The role of the technical staff will include:

- Ensuring that the school complies with the standards set out in the document "Meeting Digital and Technology Standards in Schools and Colleges, including Filtering and Monitoring standards.
- To review the school's Filtering and Monitoring process at least annually.
- To conduct an annual online safety review
- To conduct a half-termly Internet Filter test.
- Ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- Ensuring that the school meets required Online Safety technical requirements.
- Ensuring that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- Making sure they have an up to date awareness of Online Safety matters and of the current Online Safety policy and practices
- Ensuring that they report any Online Safety related issues that arise to the Online Safety Lead.

- Ensuring that the use of the network/remote access/email/School social media accounts are regularly monitored in order that any misuse/attempted misuse can be reported to the Co-Headteachers, Online Safety Lead/Data Protection Officer for investigations/action/sanction.
- To ensure that appropriate back up procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To keep up to date documentation of the school's e-security and technical procedures.
- Ensuring that they have read, understood and signed the Staff Acceptable Use Policy, Social Media & Networking Policy, Artificial Intelligence Machine Learning Policy for Staff and the Mobile Phones, Personal Devices & Imaging Policy.

Data Protection Lead:

The role of the Data Protection Lead will include:

- Taking overall responsibility for data and security.
- To ensure that all data held on pupils on the school office machines has appropriate access controls in place.
- To keep records of data breaches, SAR and FOI requests up to date.
- To ensure that data is kept in line with the Data Retention Policy and Schedule.
- To ensure that Data Protection Impact Assessments are carried out when updating systems or onboarding new technologies.
- To arrange an annual audit for GDPR with the School's Data Protection Officer, Judicium Consulting Ltd.

Teaching and Support Staff:

The role of the teaching and support staff will include:

- Ensuring they have read, understood and signed the Staff Acceptable Use Policy, Social Media & Networking Policy, Artificial Intelligence Machine Learning Policy for Staff and the Mobile Phones, Personal Devices & Imaging Policy including appendices and Data Breach policy.
- To undergo regular Online Safety and Cyber Security training as provided by the school.
- Understand their responsibilities with regards to Filtering and Monitoring within school.
- Have an up to date awareness of Online Safety matters and of the current school Online Safety
- policy and practices.
- Ensuring that they have read and understood the Data Protection Policy.
- Reporting any suspected misuse or problem to the Co-Headteachers / Online Safety Lead.
- Staff must report any data breach to the School's designated Data Protection Lead immediately, following the outlined procedures and school policy.
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- Staff should report any befriending requests from parents or pupils at the school to the Co-Headteachers / Online Safety Lead.
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- That students/ pupils understand and follow the Online Safety and acceptable use policies
- That students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- To monitor the use of digital technologies, mobile devices, smartwatches, cameras, etc… in lessons and other school activities (where allowed) and implement current policies with regard to

these devices

- In lessons where internet use is pre-planned, students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where appropriate staff may ask the Online Safety Lead / Network Manager to approve YouTube videos required for a lesson which may be automatically blocked at source due to key words being detected.

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Contracts for either Key Stage 1 or Key Stage 2 pupils.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To understand the school policy on the use of mobile phones, smart watches, digital cameras and other handheld devices.
- To understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to a member of the school community.

Parents and Carers

- To read, understand and promote the school Pupil Acceptable Use Contracts with their children.
- To access the school website in accordance with the school Acceptable Use Agreement.
- To consult with the school if they have any concerns about their child's/children's use of technology.

External Groups

- An external individual/organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school.
- To seek parental consent if the external party intends to use a pupil photograph.
- To seek parental consent if the external party requires access via video-conferencing for tele-therapy sessions.
- External professionals will ensure that children are accompanied by a member of school staff and/or parent/carer for any video-conferencing activities.

Communication:

How the policy will be communicated to staff/pupils/community:

- Policy to be posted on the school website.
- Policy to be part of an induction package for new staff.
- Acceptable Use Agreements to be read and signed to acknowledge acceptance at the beginning of every academic year.
- Acceptable Use Agreements to be issued to the whole school community on entry to school.
- Acceptable Use Agreements to be held in pupil and personnel files.

- All users will be informed that network and internet use will be monitored.
- An Online Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An Online Safety lesson will be taught at the start of each new computing unit in relation to content of the planned unit.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to Online Safety education will be given where pupils are considered to be vulnerable.
- Termly Online Safety Newsletters to be sent to parents / carers noting any particular trends.
- Online Safety Ambassadors will support pupils in raising queries to the Online Safety Lead.
- Relevant internet safety messages will be communicated to parents via Social Media where appropriate.

Handling Complaints

The school will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequence of internet access.

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the Co-Headteachers.
- All Online Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguarding Team to establish procedures for handling potentially illegal issues.
- Any issues (including consequences) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- Complaints of cyberbullying are dealt with in accordance with our Anti Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

Review and Monitoring

- The school has an Online Safety Lead who will be responsible for document ownership, review and updates.
- The policy will be reviewed annually or when significant changes occur with regard to the technologies in use within the school.
- There is wide spread ownership of the policy and it has been agreed by the SLT and approved by the Governors.
- All amendments to the school Online Safety policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil Online Safety Curriculum

This school has a clear and progressive Online Safety education programme as part of the Computing Curriculum. This covers a range of skills and behaviours appropriate to age, experience, including:

- To STOP and THINK before they CLICK
- To develop a range of strategies to evaluate and verify information before accepting accuracy.
- Awareness that an author of a website may have a particular bias or purpose and to develop skills to recognise what they may be.
- To know how to narrow or refine a search.
- To understand acceptable behaviour when using an online environment/email.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why friends online may not always be who they say they are and to understand why they must be careful online.
- To understand why they must not post personal information.
- To understand why they must not post photographs or videos without permission.
- To know not to download files.
- To have strategies to deal with receipt of inappropriate materials.
- To understand why and how some people will groom young people for sexual reasons.
- To understand the impact of cyberbullying, sexting and trolling and to know how to seek help.
- To know how to report any abuse including cyberbullying and how to seek help.
- To have an understanding of how generative Artificial Intelligence works.

Teachers

- Plan internet use carefully to ensure that it is age appropriate.
- Will remind pupils about their responsibilities, e.g. Acceptable Use Contracts.
- Model safe and responsible behaviour in their own use of technology.
- Ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights.
- Check carefully any use of Artificial Intelligence tools intended for use within the classroom or during lessons
- Ensure that staff and pupils understand the issues around aspects of the commercial use of the internet, as age appropriate.
- Do not accept friend requests from parents or children at the school.

Staff and Governor Training

- Undertake regular Online Safety and Cyber Security training.
- Ensure that staff and Governors have had GDPR Training and know how to send or receive sensitive and personal data and understand the requirements to encrypt data.
- Staff and Governors will receive termly updates with regards to Online Safety, Cyber Security and GDPR.

Parent awareness and training

This school will provide a rolling programme of advice, guidance and training for parents to ensure that principles of Online Safety behaviour are made clear, including:

To provide –

- Information leaflets and newsletters on the website.
- Demonstrations, workshops and practical sessions.
- Suggestions for safe internet use at home.
- Provision of information about national support sites for parents.
- Support for parents on using parental controls on pupils personal devices.

3. Expected Conduct and Incident Management

Expected Conduct

In this school, all users:

- Are responsible for using the school 'Computing Systems' in accordance with the Acceptable Use Policy.
- Understand the significance of misuse or access to inappropriate materials and are aware of the consequences.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to a member of the school.
- Will be expected to know and understand school policies on the use of mobile phones, smart devices, digital cameras and hand-held devices. They should also understand school policies on the taking/use of images and on cyber-bullying.
- Take time to understand new technologies and in particular familiarise themselves with the appropriate and safe use of Artificial Intelligence in the classroom.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- No member of staff is permitted to sign into another member of staff's school laptop (see Computer Misuse Act 1990).
- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile Phones, smartwatches and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones, smartwatches or other personal devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Co-Headteachers.

- Staff should not use personal devices such as mobile phones, ipads, cameras, etc… to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- The use of mobile phones, smartwatches and other personal devices by students and staff in school will be decided by the school and covered in the school Acceptable Use and Use of Mobile Phone, Personal Device and Imaging Policies.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phone, smartwatches and personal devices will not be used during lessons or formal school time by staff.
- Mobile phones, smartwatches or other personal pupil devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones, smartwatches and other personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.

Pupils Use of Personal Devices

- Mobile phones are not allowed on site or in the school buildings unless for medical reasons, i.e. blood glucose testing and arrangements will be made on a case by case basis with the Co-Headteachers.
- Any pupil that uses a mobile phone on the way to and from school must have a consent form signed by the parent.
- Pupil's mobile phones will be switched off on entering the school premises and placed in the designated box on entry to school . This box will be kept in the school office in a secure location.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the Co-Headteachers' office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- In an emergency situation if a pupil is required to contact his/her parents/carers they will be allowed to use a school owned phone with the permission of the AHT/DHT.
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Parents/Carers

- Should provide consent for pupils to use the internet, as well as other technologies, as part of the Online Safety Acceptable Use Agreement form signed on school entry.
- Parents/carers must sign a consent form allowing pupils to bring a mobile phone onto the school premises.
- Should know and understand the rules of appropriate use and their consequences.
- Know that the school does not permit parents/carers to take photographs and videos of their child/children at school events; however, on some occasions deemed acceptable by the Co-Headteachers, they will be able to take photos of their own child/children ONLY and that the school requests that photos/videos are not shared on any social networking site such a Facebook, Instagram, WhatsApp, etc.

Incident Management

How will the school respond to any incidents of concern?

- There will be strict monitoring and application of the Online Safety Policy and a differentiated and appropriate range of consequences.
- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The Online Safety Lead will report all incidents to the Data Protection Lead, who will record events and actions taken in the School GDPR incident log. Other incidents will be reported and recorded in CPOMS with the appropriate Leads notified.
- The Designated Safeguarding Lead will be informed of any Online Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- Where an incident involves any personal data, the Data Protection Lead will be immediately informed.
- The school will manage Online Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team and escalate the concern to the Police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County Online Safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the Online Safety officer to communicate to other schools in Buckinghamshire.

Cyberbullying

How will Cyberbullying be managed?

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour. This includes child on child abuse on or off the premises.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's Online Safety ethos.
- Consequences for those involved in cyberbullying may include:
    - The perpetrator will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the perpetrator refuses or is unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other consequences for pupils and staff may also be used in accordance to the schools Antibullying, Behaviour Policy or Acceptable Use Policy.
    - Parent/carers of pupils will be informed.
    - The Police will be contacted if a criminal offence is suspected.

4. Managing the Computing Infrastructure

Internet teaching and learning, access, security (virus protection) and filtering.

Teaching and Learning –

- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- The school will ensure that the copying and subsequent use of internet-derived materials by staff and pupils complies with copyright law.
- That access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Staff will provide vigilant supervision of pupils at all times as far as reasonable.
- All staff will ensure that the signed Acceptable Use Policy is implemented.
- All staff will ensure that pupils only publish within a secure environment.
- All staff will inform all users that internet use is monitored.
- All staff will preview websites before use.
- Teachers will plan internet use to match their pupil's ability.
- All staff will encourage the use of child friendly search engines where more open searches are required.
- All staff will be vigilant when conducting 'raw' image searches with pupils.
- All staff will be responsible for reporting the failures of any filtering systems within the school.
- All staff will ensure that all users know and understand the rules of appropriate use, GDPR Compliance and consequences from misuse.
- All staff should be able to provide advice and information on reporting offensive materials, abuse, bullying, etc…
- At Key Stage 1 pupils' access to the internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.

- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.
- Any pupil who repeatedly strays from the set online objective will have their internet history monitored and consequences applied if deemed necessary.

Filtering and Monitoring

The School conforms to the standards as set out in the DfE document Managing digital and technology standards for Schools and Colleges.

The Schools filtering system:

- Blocks sites that fall into such categories as pornography, race hatred, gaming, sites of an illegal nature, etc...
- Ensures educational filters are in place.
- Applies user level filtering to ensure age appropriate content.
- Ensures a healthy network through the use of anti- virus software.
- Blocks all chatrooms and social networking sites for specific purposes.
- Uses security time outs where practicable.

In addition, all computing devices provided by school for use by staff and pupils are checked regularly by the Network Manager.

Community Usage

- The school will liaise with local organisations to establish a common approach to Online Safety.
- The school will be sensitive to internet-related issues experienced by pupils out of school e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.
- The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

Network Management

The school refers to the National Protective Security Authority (NPSA) guidance for Personnel Security which can be found here: https://www.npsa.gov.uk/ongoing-personnel-security

- Day to day network management will be carried out by the School Network Manager in conjunction with Technicians provided by Bucks Schools TST for server/switching maintenance.
- Uses individual logins for all users.
- Uses guest accounts
- Has additional local network auditing software installed.
- Ensures that the System Administrator/ Network Manager is up to date with policies and services.
- Staff will use encrypted USB sticks only in an emergency if required for planning documents and resources.

To ensure that the network is used safely, this school:

- Ensures that staff read and sign the Online Safety, Acceptable Use, Social Media & Networking, Use of Mobile Device, Personal and Imaging incl. smartwatches and Artificial Intelligence and Machine Learning Policies. Following this, staff are set up with internet, email access and network access. Online access to service is through a unique, audited username and password.
- Staff access to the school's management system is controlled through a separate password for data security purposes.
- Provides pupils with a school network log-in username and password.
- Makes clear that no one should log on as another user.
- There are separate networks for both staff and pupils to save and share work.
- Requires all users to log off at the end of use.
- Scans all mobile equipment with anti-virus/spyware before it is connected to the network.
- Makes clear that staff are responsible for ensuring that any computer/laptop loaned to them by the school is used solely to support their professional responsibilities.
- Maintains equipment to ensure that Health and Safety regulations are met.
- Ensures that staff users can only access areas on the network which are relevant to their role.
- Ensures that access to the school's network resources from remote locations by staff is restricted.
- Does not allow outside agencies to access our network remotely except where there is a clear professional need.
- Makes clear responsibilities for the daily back up of financial systems and other important files.
- Has a clear disaster recovery system in place for critical data that includes a secure back-up.
- All computer equipment is installed professionally and meets health and safety standards.
- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to emails.
- Files held on the school's network will be regularly checked.
- The Co-Headteachers/Network Manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.
- A filtering and monitoring test from SWGFL is carried out by the Network Manager every half term.
- Live monitoring is carried out weekly on a Wednesday when the Firewall content is updated and at other random points during the school term. This is recorded on the Filtering and Monitoring Log.

Password Policy

- Staff and pupils must always keep their password private.
- All users have their own unique username and private passwords.
- A forced complex password policy with Two Factor Authentication or SSO is enabled for all user accounts, including but not limited, to accessing to the school network, the School Information Management System (Bromcom), CPOMS, Medical Tracker, Gmail accounts, shared google drives and any other software systems currently in use by the school.

Staff Emails

- Staff are provided with a school domain email account for professional use only.
- School emails which are accessed on personal mobile devices must be protected by biometric authentication or pin/password protected
- Access in school to personal email addresses is not permitted.
- Staff should not use personal email accounts during school hours or for professional purposes.
- Staff should never use personal email addresses to transfer staff or pupil personal data.
- Emails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Staff are not permitted to publish personal email addresses on the school website.
- Police will be contacted if staff or pupils receive an email that is considered to be particularly disturbing or breaks the law.
- The forwarding of chain messages is not permitted.
- Individual email accounts will be terminated once an employee's contract with the school has finished.
- The Network Manager will act upon any spike alerts received via the automated Gmail system.
- **Ransomware**: - staff should be wary of opening emails with attachments or links where they do not recognise the sender. (This is one of the primary entry points for ransomware attacks and may contain links or attachments that are malicious.)
- **Ransomware**: – staff should also be vigilant for any emails from recognised contacts that appear to be mis-typed, have an incorrect address or appear suspicious in any way.
- **Ransomware**: if a member of staff believes a computer has been infected it should be shut immediately and, if present, the network cable removed. This should be reported to the Network Manager at the earliest opportunity.

Pupils

- Pupils are introduced to and use email as part of a Computing Scheme of Work.
- Pupils are taught about safety and email use.
- Pupils must not give their email address to anyone outside of the school community.
- Pupils understand that email is a form of publishing where the message should be clear.
- Pupils understand and know that their emails must be authorised before they send.
- Pupils know that they must not reveal personal information.
- Pupils STOP and THINK before they CLICK.
- Pupils must immediately tell an adult if they receive an email which makes them feel uncomfortable.
- Pupils know not to respond to malicious or threatening messages.
- Pupils know not to delete malicious messages so that they can be used as evidence.
- Pupils know not to meet anyone they have met through email without having discussed the matter with an adult.
- Pupils are not allowed to forward chain mail.
- Pupils may only use approved email accounts for school purposes.
- Whole class or group email addresses will be used in primary schools for communication outside of the school.
- Excessive social email use can interfere with learning and will be restricted.
- Pupil email addresses will be used to log into Chromebooks and for access to Google Classroom.

School Website

Oak Green has a website designed to share information about the school, share excellent work and inspire pupils, parents and carers.

- The Co-Headteachers will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The contact details on the website should be the school address, email and telephone number.
- Staff or pupils' personal information must not be published.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Pupils work can only be published with the permission of their parents.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

Oak Green School also has a policy regarding the use of photographic images of children which outlines policies and procedures.

- Uploading information will be restricted to our website authorisers.

Social Networking

Please refer to the separate Social Media/Networking and Media Relations Policies.

- School social media accounts are operated by the Network Manager and staff may request information to be added to this for communication purposes and promoting community page.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their spaces to students.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff and pupils will not use any social media sites during the school day.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

School staff will ensure –

- No reference is made in social media to students/pupil's parents/carers or school staff.
- Data about pupil/staff or parents is not shared on social media.
- They do not engage in online discussions on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video conferencing

- Only school devices will be used for any form of video-conferencing, including any tele-therapy sessions conducted by external professionals.
- Staff, governors, third parties providing professional services and parents/carers will use only the recommended videoconferencing tools Microsoft Teams, Google Meet, Zoom.
- Consent for professional tele-therapy support will be obtained from parents before virtual support is provided and the child must always be accompanied by an adult during these tele-therapy sessions.
- Children may take part in class videoconferencing activities as part of a Teacher led activity only.
- Where webcams are used there will be no 1:1 learning or communications
- Where videoconferencing is taking place with either staff, third parties or children at home all parties in the household at the time must wear suitable attire and any devices used should be in appropriate communal areas, not in bedrooms.
- Children taking part in videoconferencing at home or school must be supervised by an adult
- Where videoconferencing is taking place staff should record the length, time, date and attendance of any sessions held.
- If broadcasting or recording of sessions is necessary special consideration should be given to any child who does not have photographic consent.

CCTV

- We will not reveal any recordings without permission except where disclosed to the Police as part of a criminal investigation.
- CCTV will only be provided upon request if this does not infringe data protection.
- CCTV footage is kept in accordance with the school's CCTV policy.
- Access to the school's CCTV is limited to the IT Network Manger.

How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy.

How should personal data be protected?

Personal data will be recorded, processed, transferred and made available in accordance with The Data Protection Act 2018.

Privacy policies are available to download from the school website.

5. Data Security: Management Information System Access and Data Transfer

Strategic and operational practices

At this school:

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will ensure that the filtering and monitoring policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Online Safety Lead who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team. The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Thames Valley Police or CEOPs.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.
- Staff to report any incidents where data may have been breached to the Data Protection Lead.
- We ensure that all staff are DBS checked and records are held in one central record in the school office.
- We ensure that all staff, governors, pupils and parents sign an Acceptable Use Agreement.
- We follow LA guideline for the transfer of any data.
- We require that any Protected and Restricted data be encrypted if it is removed from the school premises and limit such data removal.
- School staff with access to setting up usernames and passwords for email, network access and Learning Platforms work within the approved systems and follow the security processes for those systems.
- Staff undertake annual housekeeping to review, remove and destroy digital materials and documents which no longer need to be stored.

Technical Solutions

- Staff have secured areas on the network to store sensitive documents or photographs.
- Staff are required to lock or log out of systems when leaving their computer.
- Staff will use Google drive or Onedrive to transfer sensitive data off site.
- Members of the SLT only have access to the school network via the firewall's secure VPN.
- Restricted written material is protected in a lockable storage cabinet in a lockable storage area.
- All servers are in lockable locations and managed by the IT Network Manager.
- Paper based sensitive information is shredded.

6. Asset Disposal

- Details of all school owned hardware will be recorded in a hardware inventory.
- Details of all school owned software will be recorded in a hardware inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped or physically destroyed.
- The school will only use authorised companies who supply a written guarantee.

Online Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
Childline: www.childline.org.uk
Childnet: www.childnet.com
Click Clever Click Safe Campaign: http://www.nidirect.gov.uk/click-clever-click-safe
Cybermentors: www.cybermentors.org.uk
Digizen: www.digizen.org.uk
Internet Watch Foundation (IWF): www.iwf.org.uk
Thames Valley Police: In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Thames Valley Police via 101
Kidsmart: www.kidsmart.org.uk
Think U Know website: www.thinkuknow.co.uk
Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com
NSPCC - https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Other relevant policies:

- Behaviour policy
- Anti Bullying Policy
- Data Protection Policy
- Safeguarding Policy
- Use of Mobile phone, personal device and imaging policy including smartwatches
- Acceptable Use policy
- Social Media & Networking Policy
- Artificial Intelligence & Machine Learning Policy
- Remote Learning Policy

- (Curriculum) Computing

End to End Online Safety

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

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of the Online Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the provider.
- Next generation firewalls which detect known and unknown threats, including encrypted traffic.
- National Education Network standards and specifications.
- The Online Safety Policy and its implementation will be reviewed annually.