Online Safety Policy

Approved by:	Children's Committee	**Date:**	8 July 2024
Signed by:		(Chair)	
Last reviewed on:	July 2024		
Next review due by:	Summer 2025		

Key Details

Online Safety Officer: Miss J. Fink, ICT Co-ordinator

Designated Safeguarding Lead (s): Mrs Rebecca Farrow, Deputy Headteacher

Named Governor with lead responsibility: Mr Gary McCallum

*This policy will be reviewed **at least** annually. It will also be revised following any concerns and/or updates to national and local guidance or procedure*

This Online Safety Policy outlines the commitment of The Oaks Secondary School to safeguard members of our school community online in accordance with statutory guidance and best practice.

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

The Oaks Secondary School will deal with 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 take place out of school

1. Policy Aims

- This online safety policy has been written by Miss J Fink (ICT Co-ordinator) involving staff, learners and parents/carers, building on The Education People online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' September 2022 update, 'Working Together to Safeguard Children' (July 2022 update) and ; 'Teaching Online Safety in School', DFE guidance January 2023 update and the Durham Safeguarding Children's Partnership procedures. .
- The purpose of The Oaks Secondary School's online safety policy is to:
    - Safeguard and protect all members of The Oaks Secondary School community online.
    - Identify approaches to educate and raise awareness of online safety throughout the community.
    - Enable all staff to work safely and responsibly to role model positive behaviour online and to manage professional standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns.

- The Oaks Secondary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
    - **Content:** being exposed to illegal, inappropriate or harmful material
    - **Contact:** being subjected to harmful online interaction with other users
    - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

2. Policy Scope

- The Oaks Secondary School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- The Oaks Secondary School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- The Oaks Secondary School believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers.

- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptop, tablet or mobile phone.

2.2 Links with other policies and practices

  - This policy links with several other policies, practices and action plans including:
  - Acceptable Use Policies (AUP) and/or the Code of conduct/staff behaviour policy
  - Behaviour and discipline policy
  - Child protection policy
  - Confidentiality policy
  - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
  - Data security
  - Image use policy
  - Mobile phone and social media policies
  - Searching, screening and confiscation policy

3. Monitoring and Review

- Technology in this area evolves and changes rapidly. The Oaks Secondary School will review this policy at least annually.
  - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Senior Leadership Team will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals1 and groups within the school.

- The Designated Safeguarding Lead (DSL) Mrs Rebecca Farrow, Deputy Headteacher has lead responsibility for online safety.
- The School's ICT Co-ordinator, Miss J. Fink has been appointed as The Oaks Secondary School's Online Safety Officer. Miss Fink also teaches Computing lessons to our pupils along with a small number of other teaching staff.
- The Oaks Secondary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management:

The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.

· The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff2.

· The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

· The headteacher/senior leaders 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.

· The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.

· The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy and acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- 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 up to date required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.

- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- 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 settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the Senior Leadership Team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding and online safety.

Governors

The DfE guidance "Keeping Children Safe in Education" states:

"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"

"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".

This review will be carried out by the The Oaks Secondary School's Governors whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

· regular meetings with the Designated Safeguarding Lead / Online Safety Lead

· regularly receiving (collated and anonymised) reports of online safety incidents

· checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)

· Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards

· reporting to relevant governors group/meeting

· Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Online Safety Lead

The Online Safety Lead will:

· work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), (where these roles are not combined)

· receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments

· have a leading role in establishing and reviewing the school online safety policies/documents

· promote an awareness of and commitment to online safety education / awareness raising across the school and beyond

· liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated

· ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents

· provide (or identify sources of) training and advice for staff/governors/parents/carers/learners

· liaise with (school/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)

· receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education.

4.2 It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify and report online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.3 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures including 'Smoothwall' monitoring and filtering system, 'Senso' usage monitoring system, 'Panda Defence 360' Anti-virus/Firewall, Encryption on all portable devices and regular monitoring (daily) of staff/pupil use of The Oaks Secondary School's computer network/internet as directed by the leadership team to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Provide training to teaching staff relating to the use of the Senso classroom/pupil monitoring system
- Ensure that our filtering policy is applied, maintained and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that our monitoring systems are applied, maintained and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

4.4 It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age-appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.5 It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement and acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with learners

- The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
    - Ensuring education regarding safe and responsible use precedes internet access.

- Including online safety in Personal, Social, Health and Citizenship Education (PSHCE), Relationships and Sex Education (RSE) and computing programmes of study.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
  - Displaying acceptable use posters in all rooms with internet access.
  - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
  - Rewarding positive use of technology.
  - Implementing appropriate peer education approaches.
  - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
  - Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
  - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable Learners

- The Oaks Secondary School recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- The Oaks Secondary School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.
- When implementing an appropriate online safety policy and curriculum The Oaks Secondary School will seek input from specialist staff as appropriate, including the SENCO, Looked After Children Designated Teacher.
- All learners will/must be supervised and monitored whilst always accessing/using the internet.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
  - DCC Online Safety Training (Guest speaker as part of the schools; service level agreement)
  - Prevent training
  - Child Protection training
  - This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.

- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- The Oaks Secondary School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats.
        - This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
    - Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our school website/social media (Facebook) forum.
    - Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
    - Requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

- The Oaks Secondary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
    - Ensure that appropriate filtering and monitoring is in place, up to date and take all reasonable precautions to ensure that users can only access appropriate material.
    - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

- The Oaks Secondary School uses a wide range of technology. This includes access to:
    - Computers, laptops, tablets and other digital devices
    - Internet which may include search engines and educational websites
    - Learning platform/intranet
    - Email
    - Games consoles and other games-based technologies
    - Digital cameras, web cams and video cameras

- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

- All computer access is monitored by the school's IT Technician via the Smoothwall/SENSO Monitoring and Filtering system.
- All staff portable devices have been encrypted.
- All staff have been asked to regularly change their passwords to provided additional protection to their devices.
- Re. tablets used by pupils: these are protected via the schools filtering system (Smoothwall). 'Apple Configurator' provides additional protection to prevent pupils from downloading apps without permission.

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

- The setting will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community. (Google and Bing search engines are currently set as default on Microsoft Edge/Chrome)
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability.
  - **Key Stage 3, 4, 5**
    In some instances:
    - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.
    - Learners will use age-appropriate search engines and online tools.
    - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.
    - Learners will be appropriately supervised when using technology, according to their ability and understanding.
      We will balance children's ability to take part in age-appropriate peer activities online, with the need to detect and prevent abuse, bullying or unsafe practice by children in accordance with the national minimum standards (NMS).

With regard to the use of YouTube, this particular website can potentially contain inappropriate content for our learners. The website itself is therefore blocked to <u>all</u> learners. Teaching staff do have access to YouTube however as it can be a useful resource for teaching purposes. Staff should always ensure that they have viewed any video content that they intend to show pupils prior to the lesson to ensure that the content is appropriate. YouTube content should only be displayed/viewed on the classroom whiteboard so that it can be monitored easily and used only by staff.

7.2 Managing Internet Access

- We will maintain a written record of users who are granted access to our devices and systems.
- A written record will be maintained by the school's ICT Technician in liaison with school staff, where relevant, relating to pupils whose internet usage is of concern. This record will be published/forwarded to all staff via Office 365 whenever it is updated or has been reviewed. All staff should ensure that they read/are aware of pupils on this list and prepare alternative/differentiated work if relevant. This list will be reviewed on a regular basis in consultation with pupils/staff concerned.
- All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

7.3 Filtering and Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility

the filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

· checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced e.g. using SWGfL Test Filtering

7.3.1 Decision Making

- The Oaks Secondary School leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- Education broadband connectivity is provided through Durham County Council.
- We use '**Smoothwall**' Monitoring and Filtering system which blocks sites which can be categorised as: pornography, racial hatred, extremism, some gaming websites, chat rooms, social media (Facebook, Twitter etc) and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- We work with DCC, ICTSS and Lightspeed (*Internet Service Provider/Filtering Provider*) to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
    - Turn off monitor/screen and report the concern immediate to a member of staff.
    - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Police or CEOP.

7.3.4 Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
    - P*hysical monitoring (staff supervision of pupils using electronic devices/accessing the internet during lesson time)*
    - Realtime monitoring of internet/computer usage via the SENSO monitoring system
    - *monitoring internet and web access (reviewing logfile information – staff and pupils)*

- If a concern is identified via monitoring approaches, we will:
    - Report the incident to the BSU (Behaviour Support Unit), Online Safety Officer, DSL (if required – in line with the school child protection policy) and ICT Technician. Reports should also be logged in writing by systems such as BSU forms, CPOMS if relevant.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- A log of all internet searches is collated on a daily basis by the schools ICT Technician. Email alerts (Smoothwall Alerts) are emailed out to relevant staff on a daily basis for perusal. In instances where there are any concerns individual search details (pupil involved, date, time, keyword searched for and location) are forwarded onto the school's DSL, ICT Coordinator and BSU Manager to be dealt with and recorded. A record of <u>all</u> irregular internet searches is forwarded on to the school's ICT Coordinator and BSU Manager on a daily basis to review/act on of required.

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
    - Full information can be found in our Data Protection Policy.

7.5 Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly.
    - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
    - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
    - Regularly checking files held on our network,
    - The appropriate use of user logins and passwords to access our network.
        - Specific user logins and passwords will be enforced for all staff and pupils.
    - All users are expected to log off or lock their screens/devices if systems are unattended. All desktop and laptop computers will time out and display the locked screen after five minutes.

7.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From year 7-14, all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to:
    - Use strong passwords for access into our system.
    - Change their passwords every year (pupils) on a regular basis (staff)

- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

Reminders to follow these guidelines (regarding changing/protecting login/password details) should be forwarded onto staff on a termly basis to maintain privacy of data/documents.

7.6 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7 Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.
- Staff should ensure that pupils have been given written consent by their parents/carers to appear on any school publications, blog posts on the school website.
- All blog posts containing pupil photos/videos are checked for approval before they are posted on the school website.
- An UpToDate list of pupil permissions can be found on the Staff Shared area and Office 365. The list is updated regularly by the School Office staff.

7.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
  - The forwarding of any chain messages/emails is not permitted.
  - Spam or junk mail will be blocked and reported to the email provider.
  - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
  - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell Miss J. Fink (Online Safety Officer) or Mr. S. Dean (ICT Technician) if they receive offensive communication, and this will be recorded in our safeguarding files/records. Staff are advised to print out a copy of any inappropriate emails for record purposes.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

7.8.1 Staff email

- The use of personal email addresses by staff for any official setting business is not permitted.
  - All members of staff are provided with an email address to use for all official communication. (Durham Learning Email account operated through Office 365)

- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

7.8.2 Learner email

- All Learners at The Oaks have been provided with a Durham Learning/Office 365 account. Learners will use provided email accounts for educational purposes.
- Learners will sign an acceptable use policy and will receive regular education regarding safe and appropriate email etiquette before access is permitted. All learners are aware that their right to an email account will be revoked if at any point it is found to be misused.

7.9 Educational use of Videoconferencing and/or Webcams

- The Oaks Secondary School recognise that videoconferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits.

    - All videoconferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.
    - Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
    - Videoconferencing contact details will not be posted publicly.
    - Videoconferencing equipment will not be taken off the premises without prior permission from the DSL.
    - Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
    - Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

7.9.1 Users

- Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities.
- Learners will ask permission from a member of staff before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the learners age and ability.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote-control pages.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

7.9.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.
- If using Teams - all pupils/users will be advised that the video conference/webcam session will be recorded at the earliest opportunity. Recorded sessions will automatically be saved in staff Office 365 accounts. Staff must ensure that all pupils have logged out of the session before stopping the recording.

7.10 Management of Learning Platforms

- The Oaks Secondary School currently uses **Office 365** as its official learning platform. Although this learning platform has been available to all our pupils for some time we re-launched the use of this learning platform at the start of September 2020 to enhance the use of home learning and remote education in line with the Government's requirements to provide good quality remote education. We also use the SeeSaw App for some pupils to access learning activities remotely. (introduced October 2020) School communication with parents/carers can now be managed through an app called DOJO as well as the usual methods of face to face meeting, telephone call or email.. (Introduced Autumn 2023) Only parents/cares and staff currently at the school have access to this app and the information contained within it.
- Leaders and staff will regularly monitor the usage of the relevant Learning Platform (LP) for their classes whenever possible, including message/communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access to the LP.
- When staff and learners leave the setting, their account (including email address) will be disabled or transferred to their new establishment.
- Learners and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - If the user does not comply, the material will be removed by the site administrator.
    - Access to the LP for the user may be suspended.
    - The user will need to discuss the issues with a member of leadership before reinstatement.
    - A learner's parents/carers may be informed.
    - If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

- **Remote Learning**
- The Oaks currently use **Office 365** (formally known as Microsoft Office), and **TEAMS** to provide home learning opportunities. This can be accessed via the users' search engine or alternatively via the school's website. (Homepage – Home Learning Hub link) In addition to this some pupil groups access the **SEESAW** app for remote education/home learning tasks and activities (introduced October 2020)
- Regular staff training relating to the use of OFFICE 365/Teams should be delivered on a regular basis to ensure that all staff can use it effectively. Any new staff to the school should ensure that they have been shown how to access and use the Office 365 website. The Oaks currently deliver some staff briefings/meetings via Teams therefore all staff should attempt to familiarise themselves with its usage. In addition to this Office 365 is now the schools main communication system and this is updated regularly throughout the day. Staff should therefore login to their Office 365 account on a daily (Mon-Fri) basis to ensure that they are aware of any school news or information.
- Focussed lessons relating to the use of Office 365/TEAMS, SEESAW and DOJO should be undertaken regularly to ensure that pupils are familiar with it's use and can access the website easily. (The computing department began focussed lessons relating to the use of Office 365/Teams in September 2020 to support remote learning during the Covid-19 pandemic. In addition to this some teaching staff are now teaching lessons through Office 365 too. Focussed lessons relating to the use of SEESAW have begun with those pupil groups using the Seesaw app)
- Staff are encouraged to post work regularly for pupil access in accordance with the school's Remote Learning Policy or (due to Covid-19 pandemic) if any pupils are isolating/working from home for any reason. Work may also be assigned through this platform for pupil use in school.
- All work should be set/assigned/posted as either a **PDF**, **MS Word** or **MS PowerPoint** document to ensure that it can be viewed easily by pupils outside of the school environment on the various devices owned by pupils. That

is, a Desktop PC, laptop, Tablet device or mobile phone. (All pupils have access to MS Word and MS PowerPoint software via their Office 365 to enable successful viewing) Please note: MS Publisher documents cannot be viewed via Office 365 unless the recipient has this software installed on their computer device.

- Copyright laws and regulations should be adhered to when setting/assigning/posting pre-made documents or worksheets on this link.
- GDPR laws and regulations should be adhered to when setting/assigning/posting work/messages for pupils on this link. That is, individual pupil names, passwords etc should not be posted in this section of the website.
- TEAMS lessons/online meetings are used if staff are asked to isolate at home. Similarly, if pupils are isolating/working from home for any reason they may be able to access lessons taking place in school. (Providing that they have access to the internet and a device to view the lesson online/remotely. Please refer to the school's current Remote Education Policy for guidelines relating to setting up, participating in and recording TEAMS lessons/meetings.
- Online safety advice should be taught in lessons/posted regularly via the school's website blog in instances where pupils are expected to work from home for long periods. (For example during the initial Covid-19 Lockdown all learners were asked to access school work via the schools website. This therefore meant that all pupils were being asked to access the internet in order to view documents or complete schoolwork.) **Advice should be aimed at pupils, parents and carers** to ensure that pupils are supported and encouraged to access the pupil portal safely within the home environment.
- Please refer to the school's Remote Education Policy relating to Remote Education.

7.11 Management of Applications (apps) used to Record Children's Progress

- We currently use **Evidence for Learning (App)** and **Progression (website-based platform)** to track learners progress and share appropriate information with parents and carers.
- The Head of School is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:
    - Only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
    - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
    - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. **Social Media**

When official school social media accounts are established, there should be:

· a process for approval by senior leaders

· clear processes for the administration, moderation, and monitoring of these accounts – involving at least **two** members of staff

· a code of behaviour for users of the accounts

· systems for reporting and dealing with abuse and misuse

· understanding of how incidents may be dealt with under school disciplinary procedures.

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of The Oaks Secondary School community.
- 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; chatrooms and instant messenger.
- All members of The Oaks Secondary School community are expected to engage in social media in a positive, safe and responsible manner.
    - All members of The Oaks Secondary School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site. All access to social media websites is blocked via the school's web filtering system.
    - The use of social media during setting hours for personal use is not permitted.
    - Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of The Oaks Secondary School community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

8.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policy.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
    - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of The Oaks Secondary School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.

- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.
    - Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputy), Head of School, or ICT Co-ordinator.
    - If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy) and ICT Co-ordinator. (Please print out or take a screenshot of any friend requests/messages. This will be filed in case of any issues that may/could arise later)
- The Oaks currently has a Facebook page that enables school news to be published publicly. All staff should be aware that if they 'like' or 'share' anything from this page they may possibly make their existence on social media public to any parents/learners accessing the Facebook page. All staff are encouraged to keep their own personal social media pages/groups private where possible.

8.3 Learners Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age-appropriate sites and resources.
- We will not set up social media accounts for learners or encourage pupils to do so outside of school.
- Any concerns regarding learners' use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
    - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications.
    - How to report concerns both within the setting and externally.

8.4 Official Use of Social Media

- Prior to July 2020, The Oaks Secondary School did not provide any official social media channels of communication. However, in an attempt to reach/inform a wider audience we now have a school Facebook page (which was set up and is currently regulated by Mrs R. Dobinson, Assistant Headteacher) which can be used to inform parents/carers, pupils or the community.
- In addition to this the school also uses the school website to inform pupils, parents, carers and the community online/out of hours. This is updated regularly by staff in terms of blog updates and copies of school letters/notices can be found on the website homepage too. All posts are archived back to the initial launch of the school website.
- All content should be submitted for review in the first instance to a site administrator so that it can be checked for irregularities (appropriate content, school continuity, spelling, grammar, pupil anonymity, photographs, pupil/parent permissions etc) before being posted onto any social media website. For example, all blog posts for the school website are sent to the schools Executive Headteacher to review and she in turn posts them through her role as school website administrator.
- All school social media websites should be locked down and privacy settings enabled and regularly reviewed to ensure that comments cannot be posted by people outside of school. All forum posts should be read-only.

8.5 Monitoring of public social media

· As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.

· the school should effectively respond to social media comments made by others according to a defined policy or process.

· when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

9. Use of Personal Devices and Mobile Phones

- The Oaks Secondary School recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

9.1 Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
    - All learners are expected to hand in their mobile phones/electronic devices to appointed members of staff upon entering the school grounds in the morning. Learners are not permitted to use them at any point during the course of the school day. All mobile phones/electronic devices should be collected from the main office by individual learners at the end of the school day.
    - All members of The Oaks Secondary School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.

- All members of The Oaks Secondary School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- All members of The Oaks Secondary School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

9.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.
- Areas where staff may not use their personal mobile phones should be clearly marked via the use of posters/signage – stating 'no personal mobile phones to be used beyond this point'.
- Staff will be regularly advised to:
  - Keep mobile phones and personal devices in a safe and secure place during lesson time.
  - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
  - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
  - Not use personal devices during teaching periods.
  - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.
  - Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputy) *or ICT Co-ordinator.*
- Staff will not use personal devices:
  - To take photos or videos of learners and will only use work-provided equipment for this purpose.
  - Directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy
  - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

9.3 Learners Use of Personal Devices and Mobile Phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- The Oaks Secondary School expects learners' personal devices and mobile phones to be handed in upon entry to the school premises.
- If a learner needs to contact his/her parents or carers, they will be allowed to use a school phone.
  - Parents are advised to contact their child via the school office.
- Mobile phones or personal devices will not be used by learners during lessons or formal educational time at any point.
  - If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.
- Mobile phones and personal devices must not be taken into examinations.

- Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

- If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place.
  - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
  - Searches of mobile phone or personal devices will only be carried out in accordance with our policy.
  - Learners' mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/carer. Content may be deleted or requested to be deleted if it contravenes our policies.
  - Mobile phones and devices that have been confiscated will be released to parents or carers only.
  - If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents/carers and visitors (including volunteers and contractors) should ensure that phones are switched off/switched to silent (parents/carers/visitors/contractors) or placed in a safe secure place during the course of the school day (volunteers/supply staff)
- The use of mobile phones is not permitted in the presence of learners.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Visitors (including volunteers and contractors) who are on site for a regular or extended period will use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or Leadership Team of any breaches our policy.

9.5 Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with learners or parents/carers is required.
- School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- School mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

9.6 Use of school/personal devices off site

- If any pupil is required to take devices such as digital cameras, iPads, go-pro equipment off site to record activities/events that they are participating in off-site staff should ensure that they complete a risk assessment relating to each pupil and their use of devices.
- Staff should refrain from using personal mobile phones on school trips for photography purposes. Staff should not take photos on their personal mobile phones/devices whilst on school trips. Staff should not post on social media websites using personal mobile phones/devices whilst participating on school trips.

10. Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
    - Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

- The school will follow the NSPCC guidance on when to contact the Police available here :- https://www.npcc.police.uk/documents/Children%20and%20Young%20people/When%20to%20call%20the%20police%20guidance%20for%20schools%20and%20colleges.pdf
    - If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Service.
    - Where there is suspicion, that illegal activity has taken place, we will contact the Education Safeguarding Service or Police using 101, or 999 if there is immediate danger or risk of harm.
    - If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or Senior Leadership Team will speak with Police *or* the Education Safeguarding Service first to ensure that potential investigations are not compromised.

10.1 Concerns about Learners Welfare

- The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - The DSL (or deputy) will record these issues in line with our child protection policy.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the DCC Safeguarding Children Board thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Senior Leadership Team in accordance with the allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Online Sexual Violence and Sexual Harassment between Children

- Our setting has accessed and understood part 5 of 'Keeping children safe in education' 2024.
- The Oaks Secondary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
    - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- The Oaks Secondary School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

- The Oaks Secondary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- The Oaks Secondary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
    - If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.
    - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
        - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Kent Police first to ensure that investigations are not compromised.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

11.2 Youth Produced Sexual Imagery ("Sexting")

- The Oaks Secondary School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- The Oaks Secondary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
        - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- Act in accordance with our child protection policies and the relevant DCC Safeguarding Child Board's procedures.
- Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Store the device securely.
    - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of learners involved, including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

11.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- The Oaks Secondary School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The Oaks Secondary School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
    - We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to learners and other members of our community on our school website.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our child protection policies and the relevant DCC Safeguarding Child Board's procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform the police via 101, or 999 if a child is at immediate risk.
    - Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or the Police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL (or deputy).
- If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from the Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- The Oaks Secondary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
    - Act in accordance with our child protection policy and the relevant DCC Safeguarding Child Boards procedures.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), the police.

- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the setting provided devices, we will:
    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
    - Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the *Senior Leadership Team* is informed in line with our managing allegations against staff policy.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
- Quarantine any devices until police advice has been sought.

11.5 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at The Oaks Secondary School.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

11.6 Child Criminal Exploitation – Including County Lines

- All staff need to be aware of the indicators that a child may be at risk from or involved with Child Criminal Exploitation (CCE) and note that this can be facilitated through the use of technology. Further details are in the school's safeguarding policy.

11.7 Online Hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at The Oaks Secondary School and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Service and/or the Police.

11.8 Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.

If we are concerned that member of staff may be at risk of radicalisation online, the Senior Leadership Team will be informed immediately, and action will be taken in line with the child protection and allegations policies.

12.0 – Use of AI (Artificial Intelligence) in school

Artificial intelligence (AI) is the use of computer systems to solve problems and make decisions. It's already a part of everyday life however, the technology is developing rapidly and throwing up many new applications and challenges for schools.

- Pupils should be taught about the use of artificial intelligence in computing lessons and provided with opportunities to explore it. As part of these lessons/discussions pupils should be informed of the pros/cons of using AI. They should however be reminded that the use of AI should be kept to a minimum (only used for focussed tasks relating to the use of AI – computing lessons) and provided with rules relating to its use in school or for home learning purposes.
- Staff/pupils should be reminded regularly to never enter sensitive information into an AI online tool. (School email address, personal details such as name, address, birthdate etc)
- Staff/pupils should continue to follow our data protection principles and rules and be aware that any text entered into an AI tool is potentially being made public and possibly misused.
- As AI is still in its early days of development The Oaks have decided that all AI online tools used in school by pupils should be closely supervised to reduce the risk of misuse.

Useful Links for Educational Settings

Education Durham

- EDC/ EDA with responsibility for Online Safety. 03000265841 (
- Guidance for Educational Settings:
    - Extranet (Pupils -> safeguarding -> Online Safety) https://gateway.durhamschools.org.uk/pupils/safeguarding/Lists/Online%20Safety/Current%20Documents.aspx
    -

Durham SCB

http://www.durham-scp.org.uk/

Durham Police:

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact the Police via 101

NSPCC have produced a useful guide about detailing at what point The Police should be contacted.

https://www.npcc.police.uk/documents/Children%20and%20Young%20people/When%20to%20call%20the%20police%20guidance%20for%20schools%20and%20colleges.pdf

Prevent Officer – Steven Holden but referrals should be made through First Contact.

Other:

- ICTSS helpdesk 03000 261100
- Sharon Lewis / Carol Glasper (LADO) 03000 268838

National Links and Resources for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
  - Parent Protect https://www.parentsprotect.co.uk/ - this includes advice for parents on peer on peer abuse and how to cope if your child has got into significant trouble online.
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk
- Parentzone (Google Internet Legends) https://parentzone.org.uk/

National Links and Resources for Parents/Carers

- Internet Matters: www.internetmatters.org

This site is particularly useful for providing clear information and up-to-date advice on setting parental controls.

- Action Fraud: www.actionfraud.police.uk (This is the place to report ransomware, scams etc.)
  - CEOP:
    - www.thinkuknow.co.uk
    - www.ceop.police.uk
  - Childnet: www.childnet.com
  - Get Safe Online: www.getsafeonline.org
  - Internet Watch Foundation (IWF): www.iwf.org.uk
  - Lucy Faithfull Foundation: www.lucyfaithfull.org
  - Parent protect - advice for parents having difficulties e.g. Peer on peer abuse or Police involvement www.parentsprotect.co.uk/
  - NSPCC: www.nspcc.org.uk/onlinesafety
    - ChildLine: www.childline.org.uk
    - Net Aware: www.net-aware.org.uk
  - The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
  - UK Safer Internet Centre: www.saferinternet.org.uk

References:

- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/835733/Keeping_children_safe_in_education_2019.pdf

- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf