Online Safety Policy

2024 - 2025

Document Title	Online Safety Policy
Version number	2.0
Policy Status	Draft
Date of Issue	September 2024
Date to be revised	September 2025

Revision Log (last 6 changes)

Date	Version No	Brief detail of change
Sept 2023	1.0	Reviewed and updated with new guidance
June 2024	2.0	Reviewed and updated with new staffing and guidance

Designated Safeguarding Lead: Luke Coulson
Online Safety Coordinator: Aoife Mehigan

This policy has been constructed using the Kent County Council (KCC) online safety policy template.

1. Policy Aims

The purpose of Leigh Academy Oaks online safety policy is to:
o Safeguard and protect all members of Leigh Academy Oaks community online.
o Identify approaches to educate and raise awareness of online safety throughout the community.
o Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
o Identify clear procedures to use when responding to online safety concerns.

Leigh Academy Oaks identifies that the issues classified within online safety are considerable, and can be broadly categorised into four areas of risk:
o Content: being exposed to illegal, inappropriate or harmful material
o Contact: being subjected to harmful online interaction with other users
o Conduct: personal online behaviour that increases the likelihood of, or causes, harm.
o Commerce: risks such as online gambling, phishing/financial scams

2. Policy Scope

Leigh Academy Oaks believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online. Leigh Academy Oaks identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. Leigh Academy Oaks believes that pupils 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, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers. This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones

2.2 Links with other policies and practices
This policy links with a number of other policies, practices and action plans including:
o Anti-bullying policy
o Acceptable Use Policies (AUP)
o Behaviour and discipline policy
o Child protection policy
o Curriculum policies, such as: RSE

3. Monitoring and Review
Leigh Academy Oaks will review this policy at least annually
o 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 ensure that we 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 DSL or online safety coordinator 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 incidents, including outcomes. Any issues identified will be incorporated into the school's action planning.

4. Roles and Responsibilities
The school has appointed Mrs Aoife Mehigan to be the online safety lead. Leigh Academy Oaks 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 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 an AUP, which covers acceptable use of technology.
Ensure that suitable and appropriate filtering and monitoring systems are in place.
Work with technical staff to monitor the safety and security of school systems and networks.
Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
Support the Online safety coordinator by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 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.
Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
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 any online safety concerns, as well as actions taken, as part of the schools 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 management 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 with the governor with a lead responsibility for safeguarding and online safety.

4.3 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 AUPs.
Take responsibility for the security of school 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 online safety concerns and take appropriate action by following the school's 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.

4.4 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 password policies and encryption) to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
Ensure that the schools filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.

Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

4.5 It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:
Engage in age appropriate online safety education opportunities.
Read and adhere to the school AUPs.
Behave in a principled manner online and 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.

4.6 It is the responsibility of parents and carers to:
Read the school AUP available online and encourage their children to adhere to them.
Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
Role model safe and appropriate use of technology and social media.
Abide by the school's AUP.
Identify changes in behaviour that could indicate that their child is at risk of harm online.
Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
Use school 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 pupils
The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:
o Ensuring education regarding safe and responsible use precedes internet access.
o Including online safety in the PSHE, RSE and Computing programmes of study, as well as through the PYP inquiry lessons, covering use both at home school and home.
o Reinforcing online safety messages whenever technology or the internet is in use.
o Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
o Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The school will support pupils to read and understand the AUP in a way which suits their age and ability by:
Displaying acceptable use posters in all rooms with internet access.
Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
o Rewarding positive use of technology by pupils.
o Implementing appropriate peer education approaches.
o Using support, such as external visitors, where appropriate, to complement and support the schools internal online safety education approaches.

5.1.1 Vulnerable Pupils
Leigh Academy Oaks is aware that some pupils are considered to be 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. Resources will be adapted to address these needs either in the delivery or level of resources used. Resources are also shared with parents so they are able to discuss these issues with their

child/ren. Leigh Academy Oaks will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils. Leigh Academy Oaks will seek input from specialist staff as appropriate, including the SENCO, Child in Care Lead.

5.2 Training and engagement with staff

The school will:

Provide and discuss the online safety policy 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. This training will be included in the annual Safeguarding training for all staff.

o This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.

Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.

Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.

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

5.3 Awareness and engagement with parents and carers

Leigh Academy Oaks recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies. The school will build a partnership approach to online safety with parents and carers by:

o 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 as well as providing them with access to National Online Safety: https://nationalonlinesafety.com/enrol/oaks-primary-academy

o Drawing their attention to the school online safety policy and expectations in newsletters, letters, via social media and on our website.

o Requiring them to read the school AUP and discuss its implications with their children.

o Further information is shared with parents via the academy website: https://oaksprimaryacademy.org.uk/parents/ict-internet-safety/

6. Reducing Online Risks

Leigh Academy Oaks recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

We will:

o Regularly review the methods used to identify, assess and minimise online risks.

o Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.

o Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

o Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device. All members of the school community are made aware of the school's 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 the school's AUP and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1Classroom Use

Leigh Academy Oaks uses a wide range of technology.
This includes access to:
o Computers, laptops and other digital devices (1:1 devices from Y1-Y6 including iPads and Chromebooks)
o Internet which may include search engines and educational websites
o School learning platform/intranet
o Email
o Games consoles and other games based technologies
o Digital cameras, webcams and video cameras

All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place.
Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
The school will use age appropriate search tools, Kiddle, Google Safe Search
The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledges the source of information - this is in line with our Academic Honesty Policy.
Supervision of pupils will be appropriate to their age and ability.
o Early Years Foundation Stage and Key Stage 1 Pupils' 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 pupils' age and ability.
o Key Stage 2 Pupils will use age-appropriate search engines and online tools. Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

7.2 Managing Internet Access

There are 1:1 devices in Year 1 - Year 6. All staff, pupils and visitors will read an AUP before being given access to the school computer system, IT resources or internet.This is usually common practice at the start of the academic year with reminders given regularly when using technology.

7.3 Filtering and Monitoring

7.3.1 Decision Making

Leigh Academy Oaks has a monitoring and filtering system in place called Smoothwall. All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils from inappropriate sites and content; effective classroom management and regular education about safe and responsible use is essential.

Leigh Academy Oaks will do all we reasonably can to limit children's exposure to online harms through Academy provided devices and networks and in line with the requirements of the Prevent Duty and KCSIE, we will ensure that appropriate filtering and monitoring systems are in place (Smoothwall and Sophos systems).

7.3.2 Filtering

The school uses Smoothwall which blocks sites that are categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
The school works with Leigh Academies Trust and Smoothwall to ensure effective use and monitoring of Smoothwall to ensure the safety of our pupils and staff.

Dealing with Filtering breaches

The school has a clear procedure for reporting filtering breaches.
o If pupils discover unsuitable sites, (which have got past the Smoothwall filter) they will close the screen lid and tell a member of staff immediately.
o The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead immediately.
o The breach will be recorded on Bromcom as an Online Safety concern and escalated as appropriate.

o Parents/carers will be informed of filtering breaches involving their child. Any material that the school believes is illegal will be reported immediately to the appropriate agencies, Kent Police or CEOP as well as contacting Smoothwall to ensure the site is disallowed going forward.

7.3.4 Monitoring

The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:

o Physical monitoring (supervision), or checks on pupil devices as pupils are working.

o Smoothwall emails notifications to the DSL team

The school has a clear procedure for responding to concerns identified via monitoring approaches: All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation.

Full information can be found in the information security policy

7.5 Security and Management of Information Systems

The school takes appropriate steps to ensure the security of our information systems, including:

o Virus protection being updated regularly by the IT team

o Ensuring the files on the Google Drive are restricted and only viewed by those with the relevant permissions

o Not downloading unapproved software to work devices or opening unfamiliar email attachments.

o The appropriate use of user logins and passwords to access the school network. Specific user logins and passwords will be enforced for all but the youngest users.

o All users (pupils and staff) are expected to log off or lock their screens/devices if systems are unattended.

o Further information about technical environment safety and security can be found on the Acceptable Use Policy.

7.5.1 Password policy

All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private. From Year R all pupils are provided with their own unique username and private passwords to access school systems; pupils are responsible for keeping their password private.

We require all users to:

o Always keep their password private; users must not share it with others or leave it where others can find it.

o Not to login as another user at any time.

7.6 Managing the Safety of the School Website

The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE). The school 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 pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number. The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

Access to the website is via the LAT Webdesk and is not editable by academy staff.

7.7 Publishing Images and Videos Online

The school will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to): the Image use policy, Data security, AUPs, Codes of conduct. The academy maintains a record of pupils who cannot appear in photos or videos to be published online and this is updated regularly and shared with staff.

7.8 Managing Email

Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies, including: Confidentiality, AUPs and Code of conduct.

o The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
o School email addresses and other official contact details will not be used for setting up personal social media accounts. Members of the school community will immediately tell the DSL, Mr Luke Coulson, if they receive offensive communication, and this will be recorded in the school safeguarding files/records. Staff should not email parents/carers using their school email and instead email via the school office email address.

7.8.1 Staff
The use of personal email addresses by staff for any official school business is not permitted.
o All members of staff are provided with a specific school email address, to use for all official communication. Members of staff are encouraged to have an appropriate work life balance when responding to email.

7.8.2 Pupils
Pupils will use school provided email accounts for educational purposes. Pupils will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted. Whole-class or group email addresses may be used for communication outside of the school

7.9 Educational use of Videoconferencing and/or Webcams/live lessons
Leigh Academy Oaks recognises that videoconferencing is now a main part of school life for pupils and staff. There is a section on remote learning in our Acceptable Use Policy.
o The behaviour of pupils and staff on video calls / live lessons / recorded lessons is in line with the academy behaviour policy expectations.
o 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.
o Video conferencing equipment and webcams will be kept secure and, if necessary, locked away or disabled when not in us
o For live lessons or recordings, staff will ensure that they are in a suitable location using blurred background on Google Meet as appropriate.
oStaff will ensure that all content being delivered is appropriate, as would happen in face-to-face lessons

7.10 Management of Learning Platforms
Leigh Academy Oaks uses Google Classroom as its official learning platform for pupils.
Leaders and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular, message and communication tools and publishing facilities. Only current members of staff, pupils and parents (via the child's login) will have access to the LP. When staff and/or pupils' leave the school, their account or rights to specific school areas will be disabled or transferred to their new establishment.
Pupils and staff will be advised about acceptable conduct and use when using the LP. All users will be mindful of copyright and Academic Integrity 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:
o The user will be asked to remove any material deemed to be inappropriate or offensive.
o If the user does not comply, the material will be removed by the site administrator.
o Access to the LP for the user may be suspended.
o The user will need to discuss the issues with a member of leadership before reinstatement.
o A pupil's parent/carer may be informed.
o If the content is considered to be illegal, then the school will respond in line with existing child protection procedures.
Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

8. Social Media
8.1 Expectations
The expectations' regarding safe and responsible use of social media applies to all members of Leigh Academy Oaks community. The term social media may include (but is not limited to): blogs; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant

messenger. All members of Leigh Academy Oaks community are expected to engage in social media in a positive, safe and responsible manner, at all times.
o All members of Leigh Academy Oaks 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.

o The use of social media during school hours for personal use is not permitted.
o Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
Concerns regarding the online conduct of any member of Leigh Academy Oaks community on social media, should be reported to the school and will be managed in accordance with our Anti Bullying, Managing 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 the school Code of conduct within the AUP.

Reputation
All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they 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. This will include (but is not limited to):
o Setting the privacy levels of their personal sites as strictly as they can.
o Being aware of location sharing services.
o Opting out of public listings on social networking sites.
o Logging out of accounts after use.
o Keeping passwords safe and confidential.
o Ensuring staff do not represent their personal views as that of the school. Members of staff are encouraged not to identify themselves as employees of Leigh Academy Oaks on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also 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 with schools policies and the wider professional and legal framework.
o Information and content that staff members have access to as part of their employment, including photos and personal information about pupils 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 in the school.

Communicating with pupils and parents and carers
All members of staff are advised not to communicate with or add as ‘friends’ any current or past pupils, or current or past pupils’ family members via any personal social media sites, applications or profiles.
o Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the principal.
Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the principal. Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

8.3 Pupils’ Personal Use of Social Media
Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources. The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create

accounts specifically for children under this age. Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
Pupils will be advised:
o To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples could include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
o To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
o Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
o To use safe passwords.
o To use social media sites which are appropriate for their age and abilities.
o How to block and report unwanted communications and report concerns both within school and externally.

8.4 Official Use of Social Media
Leigh Academy Oaks's official social media channels are:
o Facebook
The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
o The official use of social media as a communication tool has been approved by the principal
o Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence. Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
o Staff use the school social media provided email address to register for and manage any official school social media channels.
o Official social media sites are suitably protected.
o Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague. Official social media use will be conducted in line with existing policies, including: Anti-bullying, Image use, Data protection, Confidentiality and Child protection.
o All communication on official social media platforms will be clear, transparent and open to scrutiny. Parents, carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

9. Use of Personal Devices and Mobile Phones
Leigh Academy Oaks recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within school.

9.1 Expectations
All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-bullying, Behaviour and Child protection. Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
o All members of Leigh Academy Oaks community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
All members of Leigh Academy Oaks 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/ 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 Leigh Academy Oaks community are advised to ensure that their mobile phones and personal devices do not contain any

content which may be considered to be offensive, derogatory or would otherwise contravene the school 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 school policy and procedures, such as: Confidentiality, Child protection, Data security and Acceptable use. Staff will be advised to:

o Keep mobile phones and personal devices in a safe and secure place during lesson time.
o Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
o Not use personal devices during teaching periods, unless permission has been given by the principal, such as in emergency circumstances. Permission must be sought in advance.
Recent updates to trust level software require two factor authentication to improve online safety and security of information. To this end, staff may be required to use their devices to access these areas.

o Ensure that any content brought 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 pupils or parents and carers - unless this has been agreed: when working from home, during periods of home learning. If staff need to use their personal devices, they must hide their caller id.

o Staff will not use personal devices, such as: mobile phones, tablets or cameras to:

- To take photos or videos of pupils and will only use work-provided equipment for this purpose. Permission must be sought from the DSL in exceptional circumstances to use a personal phone for photos.
  If a member of staff breaches the school policy, action will be taken in line with the school behaviour and allegations policy

o 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 Pupils' Use of Personal Devices and school devices

Pupils will be educated regarding the safe and appropriate use of school devices and mobile phones and will be made aware of boundaries and consequences.

Year 6 are permitted to bring mobile phones to school. Exceptions can be made to this for pupils in younger year groups with permission given from the principal on a case-by-case basis.

Leigh Academy Oaks expects pupils' personal devices and mobile phones to be handed in to the school office at the beginning of the day. If a pupil needs to contact his/her parents or carers for educational purposes or if they are unwell, this is done by a member of SLT / office.

o Parents are advised to contact their child via the school office during school hours.
o Mobile phones and personal devices must not be taken into examinations.
o Pupils 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 pupil's withdrawal from either that examination or all examinations. If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place.
o School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's Behaviour or Bullying policy, or could contain youth produced sexual imagery (sexting).
o Searches of mobile phone or personal devices will only be carried out in accordance with advice on the Government's policy. www.gov.uk/government/publications/searching-screening-and-confiscation
o Pupils' mobile phones or devices may be searched by a member of the leadership team, with the consent of the pupil or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes school policies.
o Mobile phones and devices that have been confiscated will be released to parents or carers on the same day of confiscation.
o If there is suspicion that material on a pupil'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) must use their mobile phones and personal devices in accordance with the school's Acceptable use policy and other associated policies, such as: Anti-bullying, Behaviour, Child protection and Image use. The school will ensure appropriate signage and information is displayed/ provided to inform parents, carers and visitors of expectations of use. Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy. Parents are not permitted to use mobile phones on the site and signs are displayed at various points outside.

10. Responding to Online Safety Incidents and Concerns
All members of the school 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 school procedures for reporting concerns.
o Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure. The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues. After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required. If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team. Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or Kent Police using 101, or 999 if there is immediate danger or risk of harm. If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Kent Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

10.1 Concerns about Pupils Welfare
The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
o The DSL will record these issues in line with the school's child protection policy. The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures. The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

10.2 Staff Misuse
Any complaint about staff misuse will be referred to the Principal, according to the Managing Allegations Against Staff 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 the Behaviour policy and Code of conduct.

11. Procedures for Responding to Specific Online Incidents or Concerns
11.1 Youth Produced Sexual Imagery or "Sexting"
Leigh Academy Oaks recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead. The school 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". Leigh Academy Oaks 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. The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

11.1.1 Dealing with 'Sexting'
If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:

o Act in accordance with our Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Board's procedures.
o Immediately notify the Designated Safeguarding Lead.
o Store the device securely. If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
o Inform parents and carers, if appropriate, about the incident and how it is being managed.
o Make a referral to Specialist Children's Services and/or the Police, as appropriate.
o Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
o Implement appropriate sanctions in accordance with the school's Behaviour policy, but taking care not to further traumatise victims where possible.
o 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 school 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.
o 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. The school will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.
The school will not:
o 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.
In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented on recording the incident on Bromcom.
o Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

11.2 Online Child Sexual Abuse and Exploitation
Leigh Academy Oaks 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. Leigh Academy Oaks recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead. The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers. The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally. The school will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of the school community. This is clear on the academy website.

11.2. 1 Dealing with Online Child Sexual Abuse and Exploitation
If the school are made aware of incident involving online sexual abuse of a child, the school will:
o Act in accordance with the school's Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Board's procedures.
o Immediately notify the Designated Safeguarding Lead.
o Store any devices involved securely.
o Immediately inform Kent police via 101 (or 999 if a child is at immediate risk)
o Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
o Inform parents/carers about the incident and how it is being managed.
o Make a referral to Specialist Children's Services (if required/ appropriate).
o Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
o Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary. The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
o Where possible pupils 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 the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice

immediately through the Education Safeguarding Team and/or Kent Police. If the school is 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 Designated Safeguarding Lead.
If pupils at other schools are believed to have been targeted, the school will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.3 Indecent Images of Children (IIOC)
Leigh Academy Oaks will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC). The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site. The school will take action 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 the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.

If made aware of IIOC, the school will:
o Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
o Immediately notify the school Designated Safeguard Lead.
o Store any devices involved securely.
o Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO.

If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:
o Ensure that the Designated Safeguard Lead is informed.
o Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
o Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the school devices, the school will:
o Ensure that the Designated Safeguard Lead is informed.
o Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
o Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
o 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 school devices, the school will:
- Ensure that the headteacher is informed.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
- Quarantine any devices until police advice has been sought.

11.4 Cyberbullying
Cyberbullying, along with all other forms of bullying, will not be tolerated at Leigh Academy Oaks. Any form of cyber bullying will be dealt with in accordance with our behaviour policy.

11.5 Online Hate
Online hate content, directed towards or posted by, specific members of the school community or against any protected characteristics will not be tolerated at Leigh Academy Oaks and will be responded to in line with existing school policies, including Anti-bullying and Behaviour. All members of the community will be advised to report online hate in accordance with relevant school policies and procedures. The Police will be contacted if a criminal offence is suspected. If the school is unclear on how to respond, or whether a criminal offence has

been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or Kent Police.

11.6 Online Radicalisation and Extremism

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school. If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Child protection policy. If the school is concerned that a member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with the Child protection and Allegations policies.

12. Useful Links for Educational Settings Kent Support and Guidance

Guidance for Educational Settings: o
www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
www.kentesafety.wordpress.com

KSCB: www.kscb.org.uk

Kent Police: www.kent.police.uk or www.kent.police.uk/internetsafety
In an emergency (a life is in danger or a crime in progress) dial 999.
For other non-urgent enquiries contact Kent Police via 101
Other: Kent Public Service Network (KPSN): www.kpsn.net
EiS - ICT Support for Schools and Kent Schools Broadband Service Desk: www.eiskent.co.uk

National Links and Resources

Action Fraud: www.actionfraud.police.uk
CEOP: www.thinkuknow.co.uk
www.ceop.police.uk
Childnet: www.childnet.com
Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
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