GREAT OAKS SMALL SCHOOL

SAFEGUARDING COMMUNITIES EMBRACING DIFFERENCE UNLOCKING POTENTIAL

(SAFEGUARDING)

ONLINE SAFETY & SOCIAL MEDIA POLICY 2.0

HEAD TEACHER: JULIE KELLY

CHAIR OF TRUSTEES: CLIVE BEST

Date Agreed: 29TH January 2019

Date of Next Review: January 2020

Designated Safeguarding Lead Team
Designated Safeguarding Lead:
Julie Kelly (Head Teacher)
Deputy Designated Safeguarding Leads:
Rebecca Taylor and Andy Crane (Assistant Heads)
Kerri Baker (SENCo)
Safeguarding Support Team:
Jade Laslett (Student Pastoral Mentor)
Jackie Neve (PA to the Head Teacher)
Elaine Johnson (SEN Assistant)

Chair of Trustees: Clive Best
Trustee with lead safeguarding responsibility: TBC

CONTENTS	Page

1. POLICY AIMS

- This online safety policy has been written by Great Oaks Small School, involving staff, students and parents/carers, building on the Kent County Council (KCC) online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance "Keeping Children Safe in Education" 2018 and the Kent Safeguarding Children Board procedures.

- The purpose of Great Oaks Small School's online safety policy is to:
  - Safeguard and protect all members of the Great Oaks Small 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.

- Great Oaks Small 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

- Great Oaks Small School believes that online safety is an essential part of safeguarding and acknowledges it's duty to ensure that all students and staff are protected from potential harm online.
- Great Oaks Small School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Great Oaks Small School believes that students 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 board of trustees, 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 students and parents/carers.

- This policy applies to all access to the internet and use of technology, including personal devices, or where students, 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:
  - Anti-bullying policy
  - Acceptable Use Policies (AUP)
  - Behaviour policies
  - Child protection policy
  - Confidentiality policy
  - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE)
  - Data Protection Policy and related data security policies
  - Image use policy
  - Rewards and Sanctions Policy
  - Searching, screening and confiscation policy

3. MONITORING AND REVIEW

- Great Oaks Small 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 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 Head Teacher will be informed of online safety concerns, as appropriate.
- The named Trustee for safeguarding will report on a regular basis to the Board of Trustees 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 the Head Teacher, as Designated Safeguarding Lead to be the online safety lead.
- Great Oaks Small 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 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 Code of conduct and/or 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 students to develop an age-appropriate understanding of online safety.
- Support the Designated Safeguarding Lead 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.
- 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.

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 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 safeguarding team and Board of Trustees.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.

- Meet at least termly with the trustee with a lead responsibility for safeguarding, including online safety.

4.3 Safeguarding Team *(see front page for names of current post holders):*

- **DSL** Head Teacher
- **DDSL** Assistant Head
  Assistant Head
  SENCo

- **SUPPORT TEAM:**
  Pastoral Mentor
  PA to the Head Teacher
  SEN Assistant

- The Head Teacher, Assistant Heads and SENCo meet weekly to review safeguarding cases using a RAGing system, to ascertain appropriate actions. The information is logged and safeguarding data is presented to the Board of Trustees via the Head Teacher's report, once per term.
- The Kent Children's Safeguarding Board (KCSB) procedures are used for sharing information of safeguarding cases with external agencies
- Information is shared with individual staff, as appropriate, in addition to information being shared at morning briefings and weekly staff meetings.
- The School follows advice set out in the DfE Information sharing document (July 2018)

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 students (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the School AUPs.
- 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 AUPs 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 home-school agreement and/or AUPs. 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.
- Contribute to the development of the School online safety policies.

- The School does not currently have an interactive learning platform, however information is disseminated via the School's communication systems e.g newsletters, emails and the School's website. Information includes how to stay safe, child protection and online safety links
- 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 students

- 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 students by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in the PSHE, SRE and Computing programmes of study, covering use both at school and home.
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The School will support students 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 students that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
    - Rewarding positive use of technology by students.
    - Appropriate peer education approaches are implemented through daily tutor time and weekly School Council. Specific duties are undertaken by Safety Ambassadors, selected through the School Council's democratic system.
    - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
    - Seeking student voice when writing and developing school online safety policies and practices, including curriculum development and implementation.
    - Using support, such as external visitors, where appropriate, to complement and support the Schools internal online safety education approaches.

5.1.1 Vulnerable Students

- Great Oaks Small School is aware that some students are considered to be more vulnerable online due to a range of factors such as, 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. All students enrolled at Great Oaks Small School have a profile of autism/social communication difficulties with or without high anxieties and as such are considered to be more vulnerable both on and off line.
- Great Oaks Small School will ensure that differentiated and ability appropriate online safety education, access and support is provided commensurate with our student profiles.
- Members of our Great Oaks Small School's Safeguarding Team work closely with each other in addition to working closely with external specialists including speech and language therapists, physio therapists, occupational therapists, counsellors and mental health teams as appropriate to individual students.
- Our students' needs are identified and actions taken through provision planning and according to their EHCP's, as appropriate.
- **The School's communities needs are as follows:**
    - **SAFEGUARING AWARENESS IN KENT:**
        - **CSE**: Multi-Agency Sex Exploitation (MASE)
        - **Prevent** and Channel/Radicalisation and Extremism
        - FGM
        - Peer on Peer Abuse
        - Gangs and Youth Violence
        - Online Safety

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.
    - Safeguarding information sits at the top of every weekly staff meeting agenda. Safeguarding concerns, as appropriate, are shared with staff, this includes online safety as matters arise.
    - Online safety training is delivered as part of the safeguarding training programme.

  - Each week, at staff meetings, an aspect of online safety will be focused on. This will reflect the current guidance from National Online Safety, of which the School is an accredited member.
  - The School is a member of and uses The Key, Judicium, Optimus and Andrew Hall (safeguarding.pro).
  - Senior Leaders attend KCC online safety training after which relevant information is delivered to staff as part of the safeguarding training programme.
  - This will cover the potential risks posed to students (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 students.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting students, colleagues or other members of the School community.

5.3 Awareness and engagement with parents and carers

- Great Oaks Small School 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:
  - 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 School online safety policy and expectations in newsletters, letters and on our website.
  - Requesting that they read online safety information as part of joining our school, for example, within our home school agreement.
  - Requiring them to read the School AUP and discuss its implications with their children.

6. REDUCING ONLINE RISKS

- Great Oaks Small 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 school is permitted.
    - Ensure that appropriate filtering and monitoring is in place 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 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

7.1 Classroom Use

- Great Oaks Small School uses a wide range of technology. This includes access to:
    - Computers, laptops and other digital devices
    - Internet which may include search engines and educational websites
    - Email
    - Games consoles and other games based technologies
    - Digital cameras and video cameras
- All school owned devices will be used in accordance with the School's AUP and Agreement Policy with appropriate safety and security measures in place.
- Mobile device access software is not used specifically but all mobile devices that connect through the School's network device, via the internet, are filtered through Lightspeed and require the users login and password
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Google Safe Search and CBBC safe search are system enforced

- The School will ensure that the use of internet-derived materials, by staff and students, complies with copyright law and acknowledge the source of information.
- Supervision of students will be appropriate to their age and ability. Student information will be used to identify the level at which a student will access the internet:
    - **Level 1**
        - Students' 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 students' age and ability.
    - **Level 2**
        - Students 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 students' age and ability.
    - **Level 3**
        - Students will be appropriately supervised when using technology, according to their ability and understanding.

7.2 Managing Internet Access

- The School will maintain a written record of users who are granted access to the School's devices and systems.
- All staff, students and visitors will read and sign an AUP before being given access to the School computer system, IT resources or internet.

7.3 Filtering and Monitoring

7.3.1 Decision Making

- Great Oaks Small School's trustees and leaders have ensured that the School has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The board of trustees and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The School's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's 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 students; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- The School uses Lightspeed which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
    - The School filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- The School works with Judicium to ensure that our filtering policy is continually reviewed.

Dealing with Filtering breaches

- The School has a clear procedure for reporting filtering breaches.
    - If students discover unsuitable sites, they will be required to turn off monitor/screen and report the concern immediately to a member of staff The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead.
    - The breach will be recorded and escalated as appropriate.
    - 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, such as: IWF, Kent Police or CEOP.

7.3.4 Monitoring

- The School has a clear procedure for responding to concerns identified via monitoring approaches:
    - The School's Lightspeed notification system automatically emails the IT Manager immediately if someone tries to access a prohibited site.
    - The IT Manager investigates as to whether the alert has been correctly or incorrectly classified.
        - If the information is incorrectly classified it is logged as such by the IT Manager
        - If the information is correctly classified, Safeguarding procedures are followed:
            - Reported immediately to the DSL or deputy verbally
            - A 'Green' Form is completed asap and handed to the DSL or deputy
- 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 on the staff Shared Area

7.5 Security and Management of Information Systems

- The School takes 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 the School's network,
    - The appropriate use of user logins and passwords to access the School network:
        - The user logins and passwords will be enforced for all, with the exception of those who are not capable of retaining information personal to them.
    - All users are expected to log off or lock their screens/devices if systems are unattended.

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 7, all students are provided with their own unique username and private passwords to access school systems; students are responsible for keeping their password private.
- We require all users to:
    - Use strong passwords for access into our system.
    - Change their passwords every 30 days.
    - 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.

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 Independent School Standards and Government Guidance.
- 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 students' 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 administrator account for the School website will be secured with an appropriately strong password.
- The School will post appropriate information about safeguarding, including online safety, on the School website for members of the community.

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 polices, including (but not limited to): the Image use policy, Data security, AUPs, Codes of conduct, Social media and Use of personal devices and mobile phones.

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.
    - 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.
    - 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 Designated Safeguarding Lead or a member of the Deputy Designated Safeguarding Lead Team if they receive offensive communication, and this will be recorded in the School safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked in school.
- The School's wellbeing and pastoral issues are reported on SIMs and is managed by the SENCo.

7.8.1 Staff

- The use of personal email addresses by staff for any official school business is not permitted.
    - 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, especially if communication is taking place between staff and students and parents. Parents are informed that all communication must go through the School Office whereupon calls will be diverted to the appropriate member of staff. This includes email and unless information is deemed by School as an urgent matter or concern, correspondence will be entered into between the hours of 8 am and 4 pm, term time only.

7.8.2 Students

- Students will use school provided email accounts for educational purposes.
- Students will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.9 Educational use of Videoconferencing and/or Webcams

- The School does not use videoconferencing and / or webcams

7.10 Management of Applications which Record Children's Progress

- The School uses Excel to track students' progress and information shared with students, parents/carers.
- The Head Teacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that tracking systems are appropriately risk assessed prior to use, and that they are used in accordance with GDPR and data protection legislation
- To safeguard data:
    - Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content.
    - School 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

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of The Great Oaks Small 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 Great Oaks Small School community are expected to engage in social media in a positive, safe and responsible manner, at all times.
    - All members of The Great Oaks Small 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.
- Access to social media using the School provided device and systems on site is not currently permitted.
- However, if the School decides to allow access to social media on its technological devices, staff will control access and document its procedures.
    - The use of social media during school hours for personal use not permitted unless express permission from the Head Teacher or SLT has been granted for educational purposes.
    - Staff using social media during work hours and whilst using school devices may result in disciplinary or legal action.
    - 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 the, Great Oaks Small School, community on social media, should be reported to the School 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 as part of the School Behaviour policies and 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 on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites as strictly as they can.
    - 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 School.
- Members of staff are encouraged not to identify themselves as employees of Great Oaks Small School 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.
    - Information and content that staff members have access to as part of their employment, including photos and personal information about students 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 students and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past students or current or past students' 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 Designated Safeguarding Lead and/or the Head Teacher.
    - If ongoing contact with students is required once they have left the School roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.

- Staff will not use personal social media accounts to make contact with students or parents and carers, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Head Teacher.
- Any communication from students and parents and carers received on personal social media accounts will be reported to the Schools Designated Safeguarding Lead.

8.3 Students' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to students 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 students' 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.
- Students 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. 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.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
    - 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 and report concerns both within the School, VI Form at Discovery Park and externally.

8.4 Official Use of Social Media

- *Great Oaks Small School does not use* official social media channels

9. USE OF PERSONAL DEVICES AND MOBILE PHONES

Key Stage 3 and 4

Students are not permitted to use mobile phones in school. Students can bring their phone into school and hand it into the School Office where it will be securely stored until the end of the School day. If a student is found with a mobile phone on his/her person, they will be asked to take it to the School Office. Failure to follow instructions will warrant the implementation of the Child Protection (Safeguarding);Behaviour; Rewards and Sanctions Policy.

VI Form

- Students, following an appropriate induction to the VI Form are permitted to use mobile phones at lunch and breaks times while in school providing they hand in their mobile phones during lesson times. This is to limit mobile phone addiction, help with responsible, respectful usage and maximise learning.
- Great Oaks Small School recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers, but technologies need to be used safely and appropriately within school.
- Mobile phones and personal devices are not permitted to be used in specific areas within the School time such as changing rooms, toilets and swimming pools.
- Personal devices must not be connected to the school's or Discovery Park's ICT systems without permission
- Personal equipment, including memory or data sticks, must not be connected to the school's or Discovery Park's ICT systems

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.
    - All members of The Great Oaks Small School 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 The Great Oaks Small 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/ 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 policies.
- All members of The Great Oaks Small School 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 Policy and Agreement.
    - Keep mobile phones and personal devices in a safe and secure place during lesson time, such as:
        - the pass coded Staff Room;
        - locked drawer
    - 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, unless written permission has been given by the Head Teacher, such as in emergency circumstances. It is expected that staff calls are taken in a School Office. This models good behaviour and protects students and staff from unwanted information sharing.
    - 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 students or parents and carers.
    - Any pre-existing relationships, which could undermine this, must be discussed with the Head Teacher.
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
    - To take photos or videos of students and will only use work-provided equipment for this purpose.
    - Directly with students, and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches the School policy, action will be taken in line with Staff Code of Conduct and may result in disciplinary action.

- 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 Students' Use of Personal Devices and Mobile Phones

- Students in Ks3 and Ks4 are not permitted to use mobile phones in school. Students at the 6th form site (Discovery Park) are permitted to use mobile phones at lunch and breaks times while in school providing they hand in their mobile phones during lesson times. Ks3 and Ks4 students can bring their phone into school and hand it into the SENCo Office where it will be securely stored until the end of the School day. If a student is found with a mobile phone on his/her person, they will be asked to take it to the SENCo Office. Failure to follow instructions will warrant the implementation of the appropriate Behaviour Policy and/or Rewards and Sanctions Policy.

- Students will be educated regarding the safe and appropriate use of personal devices and mobile phones.

- If a student needs to contact their parent/carer they will be allowed to do so, using the phone in the School Office or their own phone in the School Office.
  - Parents and carers are instructed to contact their child via the School Office during school hours.

- Mobile phones and personal devices must not be taken into examinations.
  - Students 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 student's withdrawal from either that examination or all examinations.

- If a student breaches the School policy by having a mobile phone or device on their person, the phone or device will be confiscated and will be held in a safe place in the School Office.
  - School staff may confiscate a student'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).
  - Searches of mobile phone or personal devices will only be carried out in accordance with the School's Searching-Screening and Confiscation Policy.
  - Students' mobile phones will not be searched by a member of staff but reported to the Senior Leadership Team who will deal with it in

compliance with Behaviour, Anti-Bullying and Child Protection (Safeguarding) policies and procedures.
  - Mobile phones and devices that have been confiscated will be released to the student at the end of the School day, parents/ carers or the Police, as appropriate.
  - If there is suspicion that material on a student'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 and agreement 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.

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 students 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 and agreement policy.

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.
  - Students, parents and carers 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 students 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 Students Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - 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 Head Teacher, according to 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 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"

- Great Oaks Small School 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".

- Great Oaks Small 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.

- 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:
    - Act in accordance with our Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Board's procedures.
    - Immediately notify the Designated Safeguarding Lead.
    - 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.
    - Carry out a risk assessment which considers any vulnerability of student(s) 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 Specialist Children's Services and/or the Police, as appropriate.
    - Provide the necessary safeguards and support for students, such as offering counselling or pastoral support.
    - Implement appropriate sanctions in accordance with the School's 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 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.
    - 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:

- 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.
- 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 students to do so.

11.2 Online Child Sexual Abuse and Exploitation

- Great Oaks Small 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.
- Great Oaks Small School 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 students, 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 students and other members of the School community on the School 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:
    - Act in accordance with the School's Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Board's procedures.
    - Immediately notify the Designated Safeguarding Lead.
    - Store any devices involved securely.
    - Immediately inform Kent police via 101 (or 999 if a child is at immediate risk)
    - Carry out a risk assessment which considers any vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.

  - Make a referral to Specialist Children's Services (if required/ appropriate).
  - Provide the necessary safeguards and support for students, such as, offering counselling or pastoral support.
  - 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.
  - Where possible students 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 students 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)

- Great Oaks Small School 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:
  - Act in accordance with the Schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
  - Immediately notify the School Designated Safeguard Lead.
  - Store any devices involved securely.

  - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO Team.

- If made aware that a member of staff or a student has been inadvertently exposed to indecent images of children whilst using the internet, the School will:
  - Ensure that the Designated Safeguard Lead 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 School devices, the School will:
  - Ensure that the Designated Safeguard Lead 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 services (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 school devices, the School will:
  - Ensure that the Head Teacher is informed.
  - Inform the Local Authority Designated Officer (LADO) Team 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 Great Oaks Small School.
- Full details of how the School will respond to cyberbullying are set out in the Anti-bullying policy which can be accessed on the School's website and from the School Office upon request.

11.5 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Great Oaks Small School 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 member of staff may be at risk of radicalisation online, the Head Teacher 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 County Council Education Safeguarding Team:

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, e-Safety Development Officer
    - esafetyofficer@kent.gov.uk Tel: 03000 415797
- Guidance for Educational Settings:
    - 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
    - Kent e–Safety Blog: 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

Designated/Responsible Staff Identified
Julie Kelly Head Teacher: **DSL**
Rebecca Taylor Assistant Head: **DDSL**
Andy Crane Assistant Head: **DDSL**
Kerri Baker SENCo:
Jade Laslett Pastoral Mentor:
Jackie Neve PA to the Head Teacher
Elaine Johnson SEN Assistant;
tbc - Safeguarding Trustee

Other Related Policies	**Date**	**Supporting Documents**	**Date**
Anti-bullying Policy		DfE statutory guidance "Keeping Children Safe in Education"	19 September 2018
Acceptable Use Policies (AUP)		Kent Safeguarding Children Board procedures.	current
Behaviour policies		DfE Information sharing advice for	(July

		safeguarding practitioners	2018)
Child protection Policy		UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'	
Confidentiality Policy			
Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE)			
Data Protection Policy and related data security policies			
Image Use Policy			
Rewards and Sanctions Policy			
Searching, Screening and Confiscation Policy			

Version Number	Purpose/Change	Author	Date Changed	Review Date
2.0	Revised Policy	KELSI & RT	22/01/2019	