The Lodge Nursery School

Online Safety policy

The Lodge Nursery believes that the use of information and communication technologies in EY settings brings great benefits. Recognising the e-Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications.

1.0. Introduction

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

This online safety policy takes into account the DfE statutory guidance 'Keeping Children Safe in Education 2018', Early Years Foundation Stage 2017, Working Together to Safeguard Children 2018 and the Kent Safeguarding Children Board procedures, and builds upon the Kent County Council / The Education People online safety policy template, with specialist advice and input as required.

2.0. Aims

The purpose of The Lodge online safety policy is to:

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

The Lodge 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.

3.0. Scope

- The Lodge believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- The Lodge identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- The Lodge believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including, leadership team, teachers/Nursery School Assistant, support staff, external contractors, visitors, volunteers and other

individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers.

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

4.0. Links with other policies and practices

- This policy links with several other policies, practices and action plans including:
- Acceptable Use Policies (AUP) and the Code of conduct/staff behaviour policy
- Behaviour and discipline policy
- Child protection policy
- Confidentiality policy
- General Data Protection Policy
- Camera and Digital Image Policy
- Mobile phone and social media policies

5.0. How will the internet be accessed at The Lodge

- **All adult users of the internet will need to agree to the Acceptable Use Policy**
- **For young users, access to the internet will only be adult demonstration or adult supervision, allowing access to specific and agreed sites only.**

6.0. Monitoring and Review

- Technology in this area evolves and changes rapidly. The Lodge will review this policy at least annually.
    - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the DSL will be informed of online safety concerns, as appropriate.
- Any issues identified via monitoring will be incorporated into our action planning.

7.0. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) has lead responsibility for online safety. Whilst activities of the designated safeguarding lead may be delegated to an appropriately trained deputy, overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL.

- The Lodge recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

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

7.2. 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.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- All ICT users are aware of the procedures that must be followed in the even to f a potentially unsafe or inappropriate online incident taking place.
- The recording and monitoring in the event of a potentially unsafe or inappropriate online incident or concern, including action taken. This should include the creation of an Incident Log (Logging a Concern Form) which should be used to inform future online safety practice. Report online safety concerns, as appropriate, to the setting management team.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.

- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually).

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

7.4. Introducing the policy to children and young people:

- Age appropriate rules and rights for internet access will be posted in areas where computers and tablets are used if they are used unsupervised.
- Children and young people will be informed that internet use is monitored. No child is left unsupervised with a tablet or laptop.
- The teaching of online safety will be part of the provision for all children and young people. It will include key messages that are age and maturity appropriate, such as keeping personal information safe, dealing with cyberbullying, knowing who to tell if there is inappropriate content / contact online (as appropriate for their age).

7.5. Introducing the policy to families and carers:

- The Lodge recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats. in newsletters, the induction pack and on the website and sharing external publications such as Digital Parenting magazine.
    - Drawing attention to our Online Safety Policy as part of the induction process.

- Parents complete agreements as part of the registration process regarding acceptable use of images and other information, for example, they agree not to download or use photos from Tapestry for any purpose other than their own viewing (see also Tapestry Policy) and that they will adhere to our Camera, Mobile Phone and Digital Images policies. .

- The Lodge works in partnership with parents. We raise awareness at meetings, in newsletters making suggestions for safe internet use at home.
- Advice on filtering systems, educational and leisure activities that include responsible use of the internet is made available to parents.
- Interested parents are referred to organisations such as CEOP, Childnet International, PIN, Parents Online and NCH Action for Children.

8.0. Education and engagement with learners

- The Lodge plans an online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
    - Children at The Lodge do not have unsupervised access to the internet
    - Supervised internet access for children will be designed for educational aspects of social and developmental use and will include age appropriate filtering.
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Age appropriate materials to support children's understanding of the risks associated with internet use and appropriate behaviour online (such as stories aimed at Early Years).
    - Practitioners should guide children in online activities that will support their developmental and learning outcomes.

- The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
    - Informing learners that internet use will be monitored for safety reasons.
    - Rewarding positive use of technology.
    - Providing age appropriate online safety education
    - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

9.0. Vulnerable Learners

- The Lodge recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- The Lodge will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.
- When implementing an appropriate online safety policy and curriculum The Lodge will seek input from specialist staff as appropriate, including the SENCO, Key Person and other support services.

10.0. Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
    - This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

11.0. Reducing Online Risks

- The Lodge recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. In common with other media such as magazines, books and DVDs, some material available via the internet is unsuitable for children and young people. The Lodge will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer or tablet. The Lodge cannot accept liability for the material accessed, or any consequences of internet access, but will uphold high standards to try to prevent it. As such, children will not be allowed unsupervised access to the internet at The Lodge.
- We will:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
    - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or

offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

12.0.Safer Use of Technology

12.1.Setting Use and Managing Internet Access

- The Lodge 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
  - Learning platform/intranet
  - Email
  - Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place. The Kindle Fire Tablets in use at The Lodge are subject to Device Management Software. This is reviewed once a month by the Setting Director.
- Members of staff will always evaluate websites, tools and apps fully before use in the setting or recommending for use at home.
- The setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
  - It is recommended that staff use one of the following: SWGfL Squiggle, Dorling Kindersley find out, Google Safe Search or CBBC safe search.
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability. Children are supervised at all times when accessing handheld devices and any other technology including cameras and computers.
  - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.

- Only our core teaching staff are granted access to our devices and systems. Volunteers are not.
- All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

12.2.Filtering and Monitoring

- Children are not granted unsupervised access to the internet.
- Access to the internet is by adult demonstration. Teachers are required to use one of the recommended search tools as above.
- The DSL will manage the permitting and banning of websites.
- Guidance on 'appropriate levels' of filtering and monitoring can be found at: *https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring*

- ***Any material that the setting believes is illegal must be referred to the Internet Watch Foundation (http://www.iwf.org.uk)***

12.2.1. Decision Making

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

12.2.2. Filtering

- Broadband connectivity is provided through BT.
- We use the security settings on Silk Browser to block sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- We ensure that our filtering policy is continually reviewed.
- If members of staff discover unsuitable sites, they will be required to:
    - turn off monitor/screen and report the concern immediate to a member of staff.
    - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy).
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Kent Police or CEOP.

12.2.3. Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
    - physical monitoring (supervision) of learners by teachers;
    - monitoring internet and web access by the Director monthly;
    - If a concern is identified via monitoring approaches DSL or deputy will respond in line with the child protection policy.

- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

12.3. Managing Personal Data Online

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

12.4. Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly.
    - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
    - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
    - Regularly checking files held on our network,
    - The appropriate use of user logins and passwords to access Tapestry. Specific user logins and passwords will be enforced for all teachers and staff.
    - All users are expected to log off or lock their screens/devices if systems are unattended.
    - Further information about technical environment safety and security can be found at:
        - Acceptable Use Policy
        - Mobile Phones Policy
        - Cameras and Digital Images Policy

12.4.1. Password policy

- All members of staff will have their own unique username and private passwords to access Tapestry. This is the only online system / network which staff have access to. Members of staff are responsible for keeping their password private.
- We require all users to:
    - Use strong passwords for access into our system.
    - 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.

12.5. Managing the Safety of our Website and Social Media Content

- Staff, children or families personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.

- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.
- Written permission from parents or carers will be obtained before photographs of children or young people under the age of 16 are published on the setting's website.
- Full names of children and young people will not be used anywhere on the website.
- Where audio or video are included, the nature of the items uploaded will not include content that allows the children and young people to be identified.

12.6. Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, General Data Protection, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

12.7. Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
  - The forwarding of any chain messages/emails is not permitted.
  - Spam or junk mail will be blocked and reported to the email provider.
  - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
  - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell the DSL if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Access to external personal email accounts and Social Media Accounts is not permitted onsite during working hours.

12.7.1. Staff email

- The use of personal email addresses by staff for any official setting business is not permitted.
  - If a situation requires it, a member of staff can be provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email. Staff do not communicate with parents by email or social media. Communication goes only through the Directors email account.

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

- We use Tapestry to track learners progress and share appropriate information with parents and carers.
- The Director is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:
  - Only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
  - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
  - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
  - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
  - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.
- The Lodge uses Tapestry Learning Journal as its official learning platform.
- Leaders and staff will regularly monitor the usage of Tapestry, including message/communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access to Tapestry.
- When staff leave the setting, their account will be disabled.
- When parents are no longer associated with the setting their accounts will be disabled.
- When children are no longer associated with the setting their accounts will be made inactive.
- Parents and staff will be advised about acceptable conduct.
- A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

13.0.Social Media

13.1.Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of The Lodge 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 Lodge community are expected to engage in social media in a positive, safe and responsible manner.
  - All members of The Lodge 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.
- The use of social media during setting hours for personal use is not permitted.

    - Use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of The Lodge community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.
- Children and young people will not be allowed to access social networking sites.

13.2.Staff Personal Use of Social Media

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

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
    - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of The Lodge on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers

- All members of staff are advised not to communicate with or add as ‘friends’ any current or past children, parents or their family members via any personal social media sites, applications or profiles.
    - Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputy) and the Director.
    - If ongoing contact with parents is required once they have left the setting, members of staff will be expected communicate via the Director using existing alumni networks or use official setting provided communication tools.
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Director.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy).

13.3.Official Use of Social Media

- The Lodge official social media channels are:
    - Facebook
    - Twitter
    - WhatsApp
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
    - The official use of social media as a communication tool has been formally risk assessed and approved by the Director.
    - Only the Director has login details for our social media channels.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
    - The Director uses setting provided email addresses to register for and manage any official social media channels.
    - No other staff have access to official social media.
    - Official social media sites are suitably protected and, where possible, linked to our website.
    - Public communications on behalf of the setting will, where deemed necessary or 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: Behaviour Management, Camera and Digital Image, General Data Protection, Confidentiality and Child Protection.
    - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Social media is not used with learners; If it ever were, written parental consent will be obtained, as required.

- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Sign our social media acceptable use policy.
    - Always be professional and aware they are an ambassador for the setting.
    - Disclose their official role but make it clear that they do not necessarily speak on behalf of the setting.
    - Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
    - Ensure that they have appropriate consent before sharing images on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, learners, parents and carers.
    - Inform their line manager, the DSL (or deputy) and/or the Director of any concerns, such as criticism, inappropriate content or contact from parents.

14.0.Use of Personal Devices and Mobile Phones

- The Lodge recognises that personal communication through mobile technologies is an accepted part of everyday life for learners (as they get older), staff and parents/carers, but use of personal devices and personal mobile phones is prohibited at The Lodge.

14.1.Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, General data protection, Mobile Phone and acceptable use.
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place in the dedicated boxes in the kitchen during session times.
    - Keep mobile phones and personal devices switched off or switched to ‘silent’ mode during session times.
    - Ensure that Bluetooth or other forms of communication (such as ‘airdrop’) are hidden or disabled during lesson times.
    - Not use personal devices during session time, unless explicit permission has been given by the Director, such as in emergency circumstances, in

    which event the use of personal device will be supervised in all areas where we care for children.
  - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting any children or parents and carers.
  - Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputy) and Director.
- Staff will not use personal devices:
  - Mobile phones and personal devices are not permitted to be used in areas where we care for children including the two halls, toilets, garden or corridors unless explicit permission has been obtained, in which case use will be supervised by another member of staff.
  - To take photos or videos of learners and will only use work-provided equipment for this purpose.
  - Directly with children and will only use work-provided equipment during lessons/educational activities. Any exception must be agreed with the Director and use will be supervised.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy
  - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

14.2. Learners Use of Personal Devices and Mobile Phones

- Children are not permitted to use any personal device at The Lodge.

14.3. 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 our acceptable use policy and other associated policies, such as digital images, mobile phones child protection and image use. Visitors are asked not to use their personal devices and mobile phones at any time when at the setting.
- We will ensure appropriate signage and information is displayed and 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 DSL (or deputy) or Director of any breaches our policy.

14.4. Officially provided mobile phones and devices

- There are work mobile phone devices on site at all times which staff can use should they need to contact parents.
- Setting mobile phones and devices will be suitably protected via a pin and must only be accessed or used by members of staff.
- Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.
- Officially provided mobile phones and other devices should be used in plain view of other staff and never taken into the toilets.

15.0. Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
  - Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, we 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 our community (for example if other local settings are involved or the public may be at risk), the DSL or Director will speak with Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

15.1. Concerns about Learners Welfare

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

15.2. Staff Misuse

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

16.0. Procedures for Responding to Specific Online Incidents or Concerns

16.1. Online Sexual Violence and Sexual Harassment between Children

- Our setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2018.
- The Lodge recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
    - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection policy.
- The Lodge recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- The Lodge also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- The Lodge will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods, mainly to engage parents.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
    - If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.

    - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
        - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Kent Police first to ensure that investigations are not compromised.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

16.2. Youth Produced Sexual Imagery ("Sexting")

- The Lodge recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- The Lodge 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, mainly engaging parents.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
        - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
    - Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures.
    - Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Store the device securely.
        - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
    - Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.

    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
    - Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
        - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
    - Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

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

- The Lodge will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The Lodge recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, but mainly staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child is at immediate risk.
    - Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.

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

16.4. Indecent Images of Children (IIOC)

- The Lodge will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.

- If made aware of IIOC, we will:
    - Act in accordance with our child protection policy and the relevant Kent Safeguarding Child Boards procedures.
    - Store any devices involved securely.
    - 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 learner has been inadvertently exposed to indecent images of children, we will:
    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.

    - Report concerns, as appropriate to parents and carers.

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

- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
    - Ensure that the DSL and Director is informed in line with our managing allegations against staff policy.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
    - Quarantine any devices until police advice has been sought.

16.5.Cyberbullying and Online Hate

- Cyberbullying, along with all other forms of bullying, will not be tolerated at The Lodge.
- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at The Lodge.
- All members of the community will be advised to report cyber bullying and online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Team and/or Kent Police.
- Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.
It is essential that young people, staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Where bullying outside the setting (such as online or via text) is reported to the setting, it should be investigated and acted on.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If staff feels that an offence may have been committed they should seek assistance from the police.

For more information please read “Preventing and Tackling Bullying: Advice for School Leaders, Staff and Governing Bodies”
http://www.education.gov.uk/aboutdfe/advice/f0076899/preventing-and-tackling-bullying

DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the Setting’s community will not be tolerated. All incidents of cyberbullying reported to the setting will be recorded.

All incidents and allegations of Cyberbullying will be investigated. Staff and parents/carers will be advised to keep a record of the bullying as evidence. Staff will take steps to identify the bully, where possible and appropriate. This may include examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Staff and parents/carers will be required to work with the setting to support the approach to cyberbullying and the setting’s e-Safety ethos.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended for the user for a period of time. Other sanctions for children and staff may also be used in accordance with anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of children will be informed.
- The Police will be contacted if a criminal offence is suspected.

16.6.Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. Internet use is strictly by adult supervision only and we use the recommended search sites as above before accessing any page.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the DSL / Director will be informed immediately, and action will be taken in line with the child protection and allegations policies.

17.0.Useful Links for Educational Settings

Kent Support and Guidance for Educational Settings
Education Safeguarding Team:

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, Online Safety Development Officer
  - 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 Online Safety Blog: www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

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 for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- 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

National Links and Resources for Parents/Carers

- 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

More detailed guidance booklets listed below, plus E-Safety Audit and CONTACTS are available on the Safeguarding file

- **S2a. Keeping Young Children Safe online**
  S2b. E-safety audit
  S2c. E-safety contacts and references
  S2d. Dealing with Cyberbullying KCC Guidance
  S2e. Cyberbullying leaflet Childnet/dfcsf guidance
  S2f. Response to an Incident of Concern KCC Flowchart
  S2g. CEOP Threat Assessment of Child Sexual Exploitation and Abuse

e-Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Staff that could contribute to the audit include: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator.

Has the school an e-Safety Policy that complies with Kent guidance?	Y/N
Date of latest update: 25 September 2018	
Date of future review: September 2019	
The policy is available for staff to access at: Safeguarding files in the cupboard onsite	
The policy is available for parents/carers to access at: Website, parent Policy file, and on request	
The responsible member of the Senior Leadership Team is: Amelia Clark	
The Designated Child Protection Coordinator is: Amelia Clark, Caroline Nokes, Heidi Guinane	
The e-Safety Coordinator is: Caroline Nokes	
Were all stakeholders (e.g. pupils, staff and parents/carers) consulted with when updating the school e-Safety Policy?	Y staff
Has up-to-date e-safety training been provided for all members of staff?	Y
Do all members of staff sign an Acceptable Use Policy on appointment?	Y
Are all staff made aware of the schools expectation around safe and professional online behaviour?	Y
Is there a clear procedure for staff, pupils and parents/carer to follow when responding to or reporting an e-Safety incident of concern?	Y
Have e-safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	Y
Is e-Safety training provided for all children (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	N/R
Are staff, children, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y staff N/R to parents
Is personal data collected, stored and used according to the principles of the GDPR	Y
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. KPSN)?	N/R
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	N/R
Does the setting log and record all e-Safety incidents, including any action taken?	Y
Are the leadership team monitoring and evaluating the setting e-Safety policy and ethos on a regular basis?	Y

e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

e–Safety Officer, Children's Safeguards Team, Families and Social Care, Kent County Council. The e-Safety Officer is Rebecca Avery email: esafetyofficer@kent.gov.uk
Tel: 01622 221469

Childline: www.childline.org.uk

Childnet: www.childnet.com

Children's Officer for Training & Development, Children's Safeguards Team, Families and Social Care, Kent County Council. The Children's Officer for Training & Development is Mike O'Connell email: mike.oconnell@kent.gov.uk Tel: 01622 696677

Children's Safeguards Team: www.kenttrustweb.org.uk?safeguards

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

EiS - ICT Support for Schools and ICT Security Advice: www.eiskent.co.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kent e–Safety in Schools Guidance: www.kenttrustweb.org.uk?esafety

Kent Police: In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 01622 690690 or contact your Safer Schools Partnership Officer. Also visit www.kent.police.uk or www.kent.police.uk/internetsafety

Kent Public Service Network (KPSN): www.kpsn.net

Kent Safeguarding Children Board (KSCB): www.kscb.org.uk

Kidsmart: www.kidsmart.org.uk

Schools Broadband Service Desk - Help with filtering and network security: www.eiskent.co.uk Tel: 01622 206040

Schools e–Safety Blog: www.kenttrustweb.org.uk?esafetyblog

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com