Online Safety Policy

Leadgate Primary School

Leadgate Primary School

Online Safety Policy

April 2022

Agreed by:

HT: Mr Watson Date: Sept 2023

Staff: Tracy Reed E Safety Coordinator Date: Sept 2023

Date for review: Sept 2024

Using the Online Safety Policy

An online safety policy provides a framework for online safety and enables strategic approaches and considerations with regards to the safer use of technology.

An online safety policy should be recognised as a safeguarding policy, not a technical or computing policy and falls within the role and responsibilities the Designated Safeguarding Lead. There is no requirement to have a separate online safety policy but this demonstrates how and where to locate safety information, especially regarding responding to and reporting specific online safety concerns.

Both Durham County Council and The Education People make every effort to ensure that the information they provide is accurate and up-to-date.

The copyright is held by The Education People but schools have been granted permission to use these materials for not for profit use.

The template for this policy has been localised with the permission of Kent County Council.

Policy statements have been individualised for our own school.

Key Details for Leadgate Primary School

Designated Safeguarding Lead (s):	**Mr Mark Watson, Head Teacher**
Named Governor with lead responsibility:	**Cllr Watts Stelling**
Date written:	**Sept 2023**
Date agreed and ratified by Governing Body:	***Spring Term 2023 - 2024***
Date of next review:	**Sept 2024**

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

Contents

1. Policy Aims

- This online safety policy has been written by Leadgate Primary School, involving staff, learners and parents/carers, building on the Kent County Council/The Education People/Durham County Council online safety policy template, with specialist advice and input given as required.
- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2021, Early Years and Foundation Stage 2021 'Working Together to Safeguard Children' 2018 and the Durham Safeguarding Children's Partnership procedures.

The purpose of Leadgate Primary School's online safety policy is to:

- Safeguard and protect all members of Leadagte Primary 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.

Leadgate Primary 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

- Leadgate Primary School believes that online safety is an essential element of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- Leadgate Primary School dentifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Leadgate Primary School believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy), as well as pupils, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.a. Links with other policies and practices

This policy links with several other policies, practices and action plans including:

- Anti-bullying Policy
- Acceptable Use Policies (AUP) and Code of conduct
- Behaviour and Discipline policy
- Class DoJo Policy
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data Protection Policy
- Mental Health and Wellbeing
- Mobile Phone contract
- Remote Learning Policy
- Safeguarding and Child Protection Policy

3. Monitoring and Review

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

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) Mark Watson has lead responsibility for online safety. *Whilst some tasks may be delegated to other appropriately trained staff, Deputy Heads Mrs Hannon and Miss Weaver, teachers Mrs Nesom and Miss Scarr, overall the ultimate lead responsibility for safeguarding and child protection, including online safety, remains with the DSL.*
- Leadgate Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.a. Key responsibilities of the school management team

- 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 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.

4.b. Key responsibilities of the Designated Safeguarding Lead (DSL)

- 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 DSL to ensure online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.

- Report online safety concerns , as appropriate, to the setting's management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet with the governor with a lead responsibility for safeguarding and online safety, at least annually.

4.c. Key responsibilities of staff

- 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.

4.d. Key responsibilities for staff managing the technical environment

- 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, such as passwords, as directed by the DSL and leadership to ensure that the setting's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

4.e. Key responsibilities of pupils (at a level that is appropriate to their individual age and ability)

- Engage in age-appropriate online safety education opportunities, e.g. Safer Internet Day. (Our school has an **online safety group** in Key Stage 2 which demonstrates that pupils have a voice in a school community approach to online safety.The Computing Coordinator aims to meet with nominated pupils from each year group every half term).
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies. ('Child-friendly' information displayed around school).
- 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.f. Key responsibilities of parents and carers

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

5. Education and Engagement Approaches

5.a. Education and engagement with pupils

- Leadgate Primary School has a progressive online safety curriculum (with links to online resources) to raise awareness and promote safe and responsible internet use amongst learners by:
    - Ensuring education regarding safe and responsible use precedes internet access
    - Including Online Safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and Computing programmes of study. (Teachers may make

    use of curriculum resources such as by Cornerstones, Teach Computing, Thinkuknow, Twinkl)
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation. Online safety is therefore included within other curriculum areas.
    - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Staff will support pupils to find out about, read and understand the acceptable use policies in a way which suits their age and ability by:
    - Displaying age-appropriate acceptable use posters in all rooms with internet access.
    - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
    - Rewarding positive use of technology where appropriate such as with certifucates or Class DoJo awards or messages.
    - Implementing appropriate peer support where appropriate
    - Seeking pupils' views and ideas when writing and developing online safety policies and practices, , including curriculum development and implementation.
    - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.b. Engagement and education of children and young people considered to be vulnerable

- At Leadgate Primary School we recognise 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.
- We aim to ensure that activities are differentiated for different abilities and additional support is provided to certain learners where appropriate, such as by using Widgit software for instructions or worksheets.
- When implementing an appropriate online safety policy and curriculum, we will seek input from specialist staff as appropriate, including the SENCO and Looked After Children Coordinator.

5.c. Engagement and training of staff

- The online safety policy and procedures will be discussed with all members of staff as part of induction.

- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff regularly, with at least annual updates. This may be during staff training days or staff meetings, as part of safeguarding and child protection training/updates or within separate or specific online safety sessions. This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.
- Staff build expertise by undertaking safeguarding training, managing safeguarding concerns and contributing to online safety procedures.
- Staff are made aware that our IT systems and internet traffic is monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Staff are made 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.
- Useful educational resources and tools, according to the age and ability of the learners, are identified.
- All members of staff are made aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

5.d. Awareness and Engagement of parents and carers

- At Leadgate Primary School we 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.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include:
    - Making information and guidance for parents available to parents in a variety of formats, such as newsletters, letters, our school prospectus and our school website
    - Highlighting online safety at other events e.g. parent evenings, transition events, fayres and sports days
    - Offering parent meetings or training with demonstrations and suggestions for safe home Internet use
    - Requesting that they read online safety information when children start our school, for example, within our home school agreement
    - Requiring them to read our acceptable use policies and discuss the implications with their children

6. Reducing Online Risks

At Leadgate Primary School we recognise 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

- Evaluate emerging technologies for educational benefit. The school leadership team will ensure that appropriate risk assessments are carried out before use in school is permitted.
- Ensure that appropriate filtering and monitoring systems are 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 *identified above.*

7. Safer Use of Technology

7.a. Classroom use

- We aim to use a wide range of technology at Leadgate Primary School. This may include access to:
    - Computers, laptops and other digital devices
    - Internet which may include search engines and educational websites
    - Class DoJo
    - Digital cameras
- All school owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place this includes whole school SMOOTHWALL filtering.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home. (A warning / disclaimer may be issued to parents regarding supervision for online content such as YouTube videos).
- The school will use age-appropriate search tools (such as ‘Swiggle’) following an informed risk assessment, to identify which tool best suits the needs of our community.
    - ***The ‘Smoothwall’ filtering system used in most Durham schools ensures that when using Google it is automatically set to safe search. This reduces but does not eliminate the risk of links to inappropriate content.***
- We will ensure that the use of internet-derived materials, by staff and learners, complies with copyright law and acknowledges the source of information.
- Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age, stage of development and ability:
    - **Early Years Foundation Stage and Key Stage 1**

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 children's age and ability.

- **Key Stage 2**
  Children will use age-appropriate search engines and online tools, and will be directed by the teacher to online materials and resources which support the learning outcomes planned for their age and ability.

7.b. Managing Internet Access

- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place. Laptops and ipads are not used by unsupervised children, mobile phones are locked away during the school day and smart watches are stored with mobile phones.
- 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.
- Pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability.
- Parents will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.

Internet use throughout the wider school/setting community

All staff, students and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

7.c. Filtering and Monitoring

A guide for education settings about establishing '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

Decision Making

- We ensured that our school has age-appropriate filtering and monitoring in place, to limit pupils' exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.

- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

Filtering

- Education broadband connectivity is provided through ***Durham County Council***
- We use ***Smoothwall*** which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. Filtering also detects other safeguarding issues, such as self-harm, serious violent crime or issues with county lines grooming.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- All school devices should be connected to a filtered feed. If a school device needs access to additional content, the filter settings for that device or user should be modified to allow access to that content. *YouTube has not been blocked as it to enable teachers to make use of educational videos.*
- We work with ***ICTSS*** to ensure that our filtering policy is continually reviewed.
- If pupils discover unsuitable sites, they will be required to:
    - Turn off their monitor/screen and report the concern immediate to a member of staff.
    - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the UK Safer Internet Centre, Durham Police or CEOP.

Monitoring

- We will appropriately monitor internet use on all school devices. This is achieved by:
    - Physical monitoring / supervision, monitoring internet and web access (reviewing logfile information)
    - Smoothwall provides reports about usage that could potentially indicate an issue which requires further investigation. Alerting e-mails are sent to The Headteacher, Mr Watson, who then takes appropriate action.
- If a concern is identified via monitoring approaches we will:
    - List how concerns will be responded to e.g. 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.

7.d. 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 (GDPR).

Full information can be found in our **Data Protection policy**

7.e. Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network. Specific user logins and passwords will be enforced for all but the youngest and some learners with SEND.
- 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 our acceptable use policy.

7.f. Password policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From Year 3, pupils are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to:
  - Use strong passwords for access into our system.
  - Change their passwords regularly (The DLG gives reminders)
  - 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.g. Managing the safety of Leadgate Primary School website

- We complete regular audits to ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or pupils' personal information will not be published on our website
- The contact details on the website will be the school/setting address, email and telephone number.
- The head teacher/manager will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The administrator accounts for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including online safety, on the school website for members of the community.

7.h. Publishing images and videos online

- The school will ensure that all images and videos shared online are used in accordance with our associated policies, including cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media, and use of personal devices and mobile phones.
- In line with our photography policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

7.i. 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.
- Members of our schol community will immediately tell Mr Watson, Head Teacher and DSL, if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

Staff email

- The use of personal email addresses by staff for any official setting business is not permitted.
- All members of staff are provided with an email address to use for all official communication.
- 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 parents.

7.j. Educational use of Videoconferencing and/or Webcams

Teachers recognise that videoconferencing and the use of webcams can be a challenging activity but can bring a wide range of learning benefits.

We may use webcams to record animals as part of science activities, such as chicks hatching or birds in a bird box, or take part in curriculum activities led by external providers such as museums.

- All videoconferencing /webcam equipment will be switched off when not in use and will not be set to auto-answer.
- Videoconferencing contact details will not be posted publicly.
- Videoconferencing equipment will not be taken off the premises without prior permission from the DSL.
- Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
- Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

Users

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

Content

- If recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.

7.k. Management of Learning Platform

- Leadgate Primary School uses Class DoJo as a learning platform.
- Only current members of staff, learners and parents will have access to this.
- When staff *or pupils* leave our school, their account will be disabled.
- Leaders and staff will regularly monitor the usage, including messages and work portfolios.
- Learners and staff will be advised about acceptable conduct and use when using it. We have a Class Dojo policy.
- All users will be mindful of copyright and will only upload appropriate content.
- Any concerns about content will be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - If the user does not comply, the material will be removed by the site administrator.
  - Access for the user may be suspended.
  - The user will need to discuss the issues with a member of leadership before reinstatement.
  - A pupil's parents/carers will be informed.
  - If the content is illegal, we will respond in line with existing child protection procedures.
- Pupils may require editorial approval from a teacher when saving work in theor portfolio.
- 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.

7.l. Management of applications (apps) used to record children's progress

- We use Edukey to share appropriate information with parents and carers of pupils identified with SEND (Special Educational Needs and Diasbilities).

- The Head Teacher and DSL, Mr Mark Watson, 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 learners' data:
  - Only school issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
  - Personal staff mobile phones or devices will NOT be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
  - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach in the event of loss or theft.
  - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
  - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

8.a. General social media use – Expectations

- The expectations regarding safe and responsible use of social media applies to all members of Leadgate Primary 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 Leadgate Primary School community are expected to engage in social media in a positive, safe and responsible manner at all times
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of of Leadgate Primary School community.
- All members of Leadgate Primary 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.
- The school will control pupil and staff access to social media and social networking sites whilst on site and when using school provided devices and systems
- The use of social media during school hours for personal use is permitted for staff during break times only.
- Inappropriate or excessive use of social media during school 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 Leadgate Primary School community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and safeguarding / child protection policies.

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

Communicating with learners and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.
    - Any pre-existing relationships or exceptions that may compromise this, will be discussed with the Head Teacher / DSL, Mr Watson (or deputy)
    - If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use official school 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 Head Teacher.
- Any communication from learners and parents received on personal social media accounts will be reported to the Head Teacher / DSL (or deputy).

8.c. Pupils' personal use of social media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age-appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13. We will not create accounts for pupils.
- Any concerns regarding pupils' use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Pupils will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications.
    - How to report concerns both within the setting and externally.

8.d. Official use of social media

Leadgate Primary School does not currently have an official social media site.

9. Use of Personal Devices and Mobile Phones

Leadgate Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within school.

9.a. Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate school policies, such as Anti-bullying, Behaviour and Child Protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
    - All members of Leadgate Primary School are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
    - All members of Leadgate Primary School 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.
- Mobile phones and personal devices are not permitted to be used in specific areas on or off site such as toilets, rooms used for changing, and swimming pools.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community; any breaches will be dealt with as part of our behaviour policy.
- All members of Leadgate Primary School are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our Behaviour or Child Protection policies.
- All members of Leadgate Primary School are reminded that taking covert images typically under clothing (Upskirting) is illegal and will be dealt with as part of the Behaviour and Discipline Policy.

9.b. Staff use of personal devices and mobile phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as relevant policy and procedures, such as: Confidentiality, Child Protection, Data Protection and Acceptable Use. (
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place, such as in a staffroom locker, during lesson time.
    - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
    - Ensure that Bluetooth or other forms of communication (such as 'Airdrop') are hidden or disabled during lesson times.
    - Not use personal devices during teaching periods, unless ***written*** permission has been given by the Head Teacher, such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are NOT permitted to use their own personal phones or devices for contacting learners or parents and carers.
    - Any pre-existing relationships, which could undermine this, will be discussed with the Head Teacher / DSL.
- Staff will not use personal devices:
    - To take photos or videos of learners and will only use work-provided equipment for this purpose.

    - Directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our Code of Conduct/staff behaviour policy
    - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence, the police will be contacted.

9.c. Pupils' use of personal devices and mobile phones

- Pupils will be taught about the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Consent must be given by parents or carers for possession of mobile phones to school
- At the start of the school day, pupils place any mobile phones and personal devices into their class box. Boxes are then kept in a secure place in the school office until the end of the school day.
- Mobile phones or personal devices belonging to pupils will not be used by pupils during lessons or educational time, or taken into any examinations.
    - Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school office phone
- Parents are advised to contact their child via the school office
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the schools behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
- Confoscated phones will be held in a secure place in the school office.
- Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the school day
- Searches of mobile phone or personal devices will only be carried out by a member of the leadership team, with the consent of a parent/carer. www.gov.uk/government/publications/searching-screening-and-confiscation)

  If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.d. 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: Anti-bullying, Behaviour, Child Protection and Photography.
- 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 Head Teacher / DSL (or deputy) of any breaches of our policy.

9.e. Officially provided mobile phones and devices

- Members of staff will be issued with a work email address.
- Teachers will also be given a work phone number, where contact with parents/carers is required.
- Setting mobile phones and devices will be suitably protected via a passcode/password/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.

10. Responding to Online Incidents and Safeguarding Concerns

- All members of the school 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 pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- The school will follow the NSPCC guidance on when to contact the Police available here: https://www.npcc.police.uk/documents/Children%20and%20Young%20people/When%20to%20call%20the%20police%20guidance%20for%20schools%20and%20colleges.pdf
- If 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 Head Teacher / DSL will speak with Durham Police first to ensure that potential investigations are not compromised.

10.a. Concerns about Pupil Welfare

- The Head Teacher / 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 Head Teacher / DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the DSCP thresholds and procedures.

- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

10.b. Staff Misuse

- Any complaint about staff misuse will be referred to the Head Teacher, in accordance with the Safeguarding Policy.
- Issues which do not meet the threshold requiring reporting to the LADO (Local Authority Designated Officer) will be recorded in the schools record of low level concerns.
- Any allegations regarding a member of staff's online conduct reaching the threshold will be discussed with the LADO.
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

11. Responding to Specific Online Incidents or Concerns

11.a. Online Sexual Violence and Sexual Harassment between Children

- Our school has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2021) guidance and part 5 of 'Keeping children safe in education' 2021.
- We recognise 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.
- We recognise that the 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.
- We also recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the Head Teacher / DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.

- If content is contained on pupils' 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 First Contact 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 Durham 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.

Youth Produced Sexual Imagery ("Nudes")

- Leadgate Primary School recognises youth produced sexual imagery (known as "nudes") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- This section only applies to YP under the age of 18 creating/sharing/receiving nudes of a YP. It does not apply to children sharing adult pornography.
- On any occasion when an adult is in possession of or is sharing an illegal image of a YP, this will always be an urgent police matter.
- We will follow the advice set out by UKCIS here https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people a summary of the guidance is now an appendix of the school safeguarding policy.
- We 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 resources such as those identified in our Digital Literacy, PSHE and RSE curriculums.
- 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 review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

11.b. Online Child Sexual Abuse and Exploitation

- Leadgate Primary 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.
- We recognise 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 Head Teacher / DSL (or deputy).
- Schools are reminded that a criminal offence has been committed if a person aged 18 or over intentionally communicates with a child under 16, who the adult does not reasonably believe to be 16 or over, if the communication is sexual or if it is intended to encourage the child to make a communication which is sexual. The offence will be committed whether or not the child communicates with the adult. This is the offence of sexual communication with a child under section 67 of the Serious Crime Act 2015.
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- The 'Click CEOP' report button is visible and available to members of our community on the home page of our school website.
- If made aware of incident involving online child sexual abuse, we will:
    - Act in accordance with our Child Protection policies and the relevant Durham SCP procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to First Contact (if required/appropriate) and immediately inform Durham 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 Head Teacher / DSL (or deputy) will obtain advice immediately through the Education Durham or Durham Police.
- If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Durham Police and/or Education Durham first to ensure that potential investigations are not compromised.

Child Criminal Exploitation – Including County Lines

All staff need to be aware of the indicators that a child may be at risk from, or involved with Child Criminal Exploitation (CCE) and note that this can be facilitated through the use of technology. Further details are in the schools Safeguarding Policy.

11.c. Indecent Images of Children (IIOC)

- Leadgate Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the Head Teacher / DSL (or deputy) will obtain advice immediately through Durham 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 Durham SCP procedures.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as CEOP, Durham 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 First Contact
    - 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 Head Teacher is informed in line with our managing allegations against staff policy.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
    - Quarantine any devices until police advice has been sought.

11.d. Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at Leadgate Primary School.

Full details of how we will respond to cyberbullying are set out in our Anti-bullying Policy, which can be found on our school website.

11.e. Online Hate

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

11.f. 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. The schools SMOOTHWALL filter will report all activitiy to the designated Senior Leader on a daily and immediate basis.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the Head Teacher / 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 Head Teacher will be informed immediately, and action will be taken in line with the Child Protection policies.

12. Useful Links

Education Durham
Paul Hodgkinson, EDA with responsibility for Online Safety
paul.hodgkinson@durham.gov.uk

03000265841

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

Durham Police:
In an emergency (a life is in danger or a crime in progress), dial 999
For other non-urgent enquiries, contact the Police via 101
NSPCC have produced a useful guide about detailing at what point the Police should be contacted:
https://www.npcc.police.uk/documents/Children%20and%20Young%20people/When%20to%20call%20the%20police%20guidance%20for%20schools%20and%20colleges.pdf
Prevent Officer: Steven Holden - but referrals should be made through First Contact.

Other:

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

National Links and Resources for Educational Settings

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

National Links and Resources for Parents/Carers

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