Timothy Hackworth Primary School

'Respectful and resilient; being the best that we can be.'

Online Safety Policy

CRC Article 19: All children have the right to be safe.

CRC Article 17: All children have the right to information.

Date of Policy: March 2022

Review date: March 2023

Date policy approved/adopted:	**March 2022**
Next review date:	**March 2023**
Approved by:	**Governing Body**
Head Teacher Signature:	*L. Boulton*
Governor Signature:	*P. Crook*

Online Safety Policy

CRC Article 19: All children have the right to be safe.

CRC Article 17: All children have the right to information.

Designated Safeguarding Lead:	Mrs. L. Boulton (Head Teacher)
Deputy Designated Safeguarding Leads:	Mrs. J. Slattery (Deputy HT) Mrs. K. Kozlowski (SENDCO) Miss N. Stainsby Mrs. B. Mathwin
Safeguarding Governor:	Mrs. P. Crook
Online Safety Lead:	Mrs. L. Boulton (Head Teacher)
Computing Lead:	Miss A. Begum
Date of Policy:	March 2022
Review Date:	March 2023

This policy should be read in conjunction with our Safeguarding Policy, Respectful Relationships Policy (Behaviour Policy), PSHE including Relationships Education Policy, and Keeping Children Safe in Education, September 2021. All policy and practice in Timothy Hackworth Primary School respects children's dignity.

Our Timothy Hackworth School Vision

May our Rights Respecting School be a happy place for us all to learn; where every one of us is valued and safe in our Timothy Hackworth School Family. May we all be the best that we can be by making a positive difference to each other, our community in Shildon and the wider world in which we all live.

Mission Statement (written by children):

We would like our school, which reflects British Values, to be at the heart of the community, sharing, supporting and learning together with everyone as equals. Our children have the right to high quality learning experiences to help them to be the best that they can be.

We encourage our children to be creative, unique, open-minded and independent individuals, respectful of themselves and of others in our school, our local community and the wider world.

We aim to nurture our children on their journey through life so that they can grow into safe, caring, democratic, responsible and tolerant adults who make a positive difference to British Society and to the world.

Values

Ours is a happy school with high hopes and ambitions for all our children and we welcome working in partnership with parents and carers to ensure that everything is done in the best interests of the children at all times.
All of our staff take their responsibility towards the children seriously and they strive to help each child reach their full potential as global citizens physically, emotionally, socially and academically. We are fully committed to the UNITED NATIONS CONVENTION ON THE RIGHTS OF THE CHILD.
To us, every child is unique and precious and we endeavour to foster a high level of motivation towards learning and behaviour. We are committed to the basic skills of English and Maths.

Equalities Information

This policy should be read in conjunction with our school's 'Equalities Policy Statement', 'Equalities Objectives Summary' and 'Equalities Information and Objectives'.

We welcome our duties under the Equality Act 2010 to eliminate discrimination, advance equality of opportunity and foster good relations in relation to age (as appropriate), disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation (LGBTQ+).

Rationale

Timothy Hackworth Primary School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online. We also acknowledge that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. We believe that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
This policy applies to all staff including the Governing Body, Leadership Team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as 'staff' in this policy) as well as learners, parents and carers.
This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided

with setting-issued devices for use off-site, such as work laptops, tablets or mobile phones.

1. Policy Aims

- This Online Safety Policy has been written, using the Kent County Council/The Education People/Durham County Council Online Safety Policy template, with specialist advice and input 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 our Timothy Hackworth Primary School Online Safety Policy is to:
  - safeguard and protect all members of Timothy Hackworth 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.
- Timothy Hackworth 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

- Timothy Hackworth Primary School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- Timothy Hackworth Primary School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Timothy Hackworth 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 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 work laptops, tablets or mobile phones.

a. Links with other policies and practices

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

- Anti-Bullying Policy;
- Staff Acceptable Use Policy (AUP) and the Staff Code of Conduct;
- Respectful Relationships (Behaviour) Policy;
- Safeguarding Policy;
- Personal Social and Health Education (PSHE), Relationships Education and Health, including Relationships and Sex Education Policy;
- Pupils' Online Safety Agreement;
- Computing Policy.

Monitoring and Review

- Technology in this area evolves and changes rapidly. Timothy Hackworth Primary School will review this at least annually.
  - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to our school's technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- 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.

3. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL), Lynn Boulton, Head Teacher, has lead responsibility for online safety. Whilst activities of the Designated Safeguarding Lead may be delegated to our school's team of Deputy Designated Safeguarding Leads, overall, the ultimate lead responsibility for safeguarding and child protection, including online safety, remains with the Designated Safeguarding Lead.

- Timothy Hackworth Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

a. The Leadership 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 and a Staff Acceptable Use Policy.
- 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 purposeful curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring that 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.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

b. 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 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 that they understand the unique risks associated with online safety and have the relevant up to date knowledge required to keep learners safe online.
- Access regular and appropriate training and support to ensure that 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 Leadership Team and Governing Body.
- Review and update online safety policies on a regular basis (at least annually).
- Meet with the Safeguarding Governor on a termly basis to provide updates as appropriate.

c. It is the responsibility of all members of staff to:

- 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, routinely.
- 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 our school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

d. It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to DSLs and the Leadership Team as appropriate, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures as directed by the DSL and Leadership Team, for example, use of passwords and encryptions, to ensure that our 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.
- Ensure that our monitoring systems are applied and updated on a regular basis.

- Ensure appropriate access and technical support is given to the Head Teacher and School Business Manager, to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if and when required.

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

- Engage in age appropriate online safety education opportunities.
- 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.

f. It is the responsibility of parents and carers to:

- 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.
- 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.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

4. Education and Engagement Approaches

a. Education and engagement with learners

- Our setting will establish and embed a purposeful online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
  - Ensuring education regarding safe and responsible use precedes internet access.
  - Including online safety in PSHE, including Relationships Education and Relationships and Sex Education (RSE), and Computing.
  - Reinforcing online safety messages whenever technology or the internet is in use.
  - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.

- Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The setting will support learners to read and understand the Acceptable Use policies in a way which suits their age and ability by:
  - Informing learners that network and internet use will be monitored for safety and security purposes.
  - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

b. Vulnerable Learners

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

c. 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, updates as part of our routine safeguarding CPD and Briefing Updates.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.

- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

d. Awareness and engagement with Parents and Carers

- Timothy Hackworth Primary School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We foster a partnership approach to online safety with parents and carers by:
  - Providing information and guidance on online safety in a variety of formats.
    - This will include offering specific online safety awareness training and highlighting online safety at other events such as parent meetings and events.
  - Drawing their attention to the Online Safety Policy and expectations in newsletters, letters, our prospectus and on our website.
  - Requesting that they read online safety information as part of joining our community, for example, as part of our Timothy Hackworth Pupils' Online Safety Agreement.
  - Requiring them to read our Pupils' Online Safety Agreement, our Home School Agreement, and to discuss the implications with their children.

5. Reducing Online Risks

- Timothy Hackworth Primary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
  - Regularly review the methods used to identify, assess and minimise online risks.
  - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
  - Ensure that appropriate filtering and monitoring is in place 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 Staff

Acceptable Use Policies and Timothy Hackworth Pupils' Online Safety Agreement, and highlighted through a variety of education and training approaches.

6. Safer Use of Technology

a. Classroom Use

- Timothy Hackworth Primary School uses a wide range of technology. This includes access to:
  - Computers, laptops, tablets and other digital devices;
  - Internet, which may include search engines and educational websites;
  - Office 365 Platform;
  - Email.
- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
  - The Durham County Council Smoothwall filtering system used in our school 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.
- Supervision of learners will be appropriate to their age and ability.

b. Managing Internet Access

- All staff and visitors will read and sign our Staff Acceptable Use Policy before being given access to our computer system, IT resources or Internet.
- Our Timothy Hackworth Pupils' Online Safety Agreement is read and signed by parents and carers and shared with children at school, and at home.

c. Filtering and Monitoring

i Decision Making

- Timothy Hackworth Primary School governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learners' 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 Head Teacher; all changes to the filtering policy are logged and recorded.
- The Head Teacher and School Business Manager 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.

ii 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. Our school is also aware of the filtering detecting 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.
- We work with ICTSS to ensure that our filtering system is continually reviewed.

- If learners discover unsuitable sites, they will be required to:
  - turn off the monitor/screen and report the concern immediately to a member of staff.
  - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy), who will inform the School Business Manager and School Engineer.
  - The breach will be recorded and escalated as appropriate.
  - Parents and 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.

iii Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
  - Physical monitoring (supervision), monitoring internet and web access;
  - Our filtering system, Smoothwall, provides reports about usage that could potentially indicate an issue which requires further investigation. Alerting e-mails are sent to the School Business Manager and School Engineer, who then immediately inform the Head Teacher, who would take appropriate action.
- If a concern is identified via monitoring approaches we will:
  - Investigate the concerns in line with our Safeguarding and Online Safety policies. The Head Teacher (DSL) and Deputy DSLs would further explore the issues and take appropriate actions.
- 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.

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.
  - Further information can be found in our Data Protection Policy.

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 are in place for all children from Year 1 upwards.
  - All users are expected to log off or lock their screens/devices if systems are unattended.

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 1, all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to:
  - Use strong passwords for access into our system;
  - 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.

g. Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learners' 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.

h. 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), camera and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

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 our Acceptable Use Policy, and the Staff Code of Conduct Policy.
  - 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 inform the Head Teacher if they receive offensive communication, and this will be recorded in our safeguarding files/records.

i 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, learners and parents.

ii Learner Email

- Learners sign a Timothy Hackworth Pupils' Online Safety Agreement, and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the setting.

j. Educational use of Videoconferencing and Webcams

- Timothy Hackworth Primary School recognises that videoconferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits.
  - All videoconferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.
  - Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.

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

iii Users

- Parents' and carers' consent will be obtained prior to learners taking part in videoconferencing activities.
- Learners will ask permission from a member of staff before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the learners' age and ability.
- Videoconferencing 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.

iv Content

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

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

- The Head Teacher 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.

7. Social Media

a. Expectations

- The expectations regarding safe and responsible use of social media applies to all members of the Timothy Hackworth 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 the Timothy Hackworth Primary School community are expected to engage in social media in a positive, safe and responsible manner.
  - All members of the Timothy Hackworth 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.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site.
  - The use of social media during setting hours for personal use is only permitted during staff lunchtimes, in the Staff Room setting only.
  - Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Concerns regarding the online conduct of any member of Timothy Hackworth 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 child protection policies.

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 Staff Code of Conduct and as part of our Staff 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 Timothy Hackworth 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.
    - If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, 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.

c. Learners' Personal Use of Social Media

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

- **Official Use of Social Media**
- **Timothy Hackworth Primary School official social media channels are:**
    - Timothy Hackworth Primary School Facebook page.
- 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 Head Teacher.
    - The School Business Manager and Parent and Family Intervention Support Lead have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
    - Staff use setting provided email addresses to register for and manage any official social media channels.
    - Official social media sites are suitably protected and, where possible, run and linked to our website.
    - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: anti-bullying, image/camera use, 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.
    - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
- Parents and carers will be informed of any official social media use with learners; 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 professional 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 and position 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 the Head Teacher of any concerns, such as criticism, inappropriate content or contact from learners.

8. Use of Personal Devices and Mobile Phones

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

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 policies, such as our Anti-Bullying Policy, Behaviour (Respectful Relationships) Policy and Safeguarding Policy.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
  - All members of Timothy Hackworth Primary School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
  - All members of Timothy Hackworth Primary School community are advised to use passwords/pin numbers to ensure that unauthorised calls

or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as toilet facilities.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour (Respectful Relationships) Policy.
- All members of Timothy Hackworth Primary School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our Behaviour (Respectful Relationships) Policy and Safeguarding Policy.
- All members of Timothy Hackworth Primary School community are reminded that taking covert images typically under clothing (Upskirting) is illegal and will be dealt with as part of the Discipline Policy.

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 Reporting, Safeguarding, Data Protection and Acceptable Use policies.
- Staff will be advised to:
  - Keep mobile phones and personal devices in designated staff lockers during lesson time.
  - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
  - Not use personal devices during teaching periods, unless 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.
- 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 staff Code of Conduct 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.

c. Learners' Use of Personal Devices and Mobile Phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Timothy Hackworth Primary School expects learners' personal devices and mobile phones to be left at home, and not to be brought into school;
- Should a child bring a mobile phone with them to school for emergency purposes only, or if they have forgotten to leave their mobile phone at home, their mobile phone would be handed into the School Office and stored in the school safe until the end of the day;
- If a learner breaches the policy, the phone or device will be confiscated and will be held in the school safe.
  - Staff may confiscate a learner's mobile phone or device;
  - Searches of mobile phone or personal devices will only be carried out in accordance with the Government's 'Searching, Screening and Confiscation' guidance: www.gov.uk/government/publications/searching-screening-and-confiscation);
  - Learners' mobile phones or devices may be searched by a member of the Leadership Team, with the consent of the learner or a parent/carer. Content may be deleted or requested to be deleted, if it contravenes our policies. www.gov.uk/government/publications/searching-screening-and-confiscation);
  - Mobile phones and devices that have been confiscated will be released to parents or carers by the end of the day;
  - 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.

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: Anti-Bullying, Behaviour (Respectful Relationships) and Safeguarding.

- Parents, carers and visitors are aware of the above policies and the related use of personal devices and mobile phones.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Head Teacher of any breaches of our policy.

- **Officially provided mobile phones and devices** Members of staff will be issued with a work phone number and email address, where contact with learners or parents and 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: Anti-Bullying, Behaviour (Respectful Relationships) and Safeguarding.

9. 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 are aware of our Complaints Procedure and staff are aware of our Confidentiality Reporting Code.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- The school will follow the NSPCC guidance on when to contact the Police - available here: https://www.npcc.police.uk/documents/Children%20and%20Young%20people/When%20to%20call%20the%20police%20guidance%20for%20schools%20and%20colleges.pdf
- If 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 will speak with Durham Police first to ensure that potential investigations are not compromised.

a. 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 Safeguarding Policy.
- The 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.

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 will be recorded in our school's record of Low Level Concerns.
- Any allegations regarding a member of staff's online conduct reaching the threshold will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff Code of Conduct.

10. Procedures for Responding to Specific Online Incidents or Concerns

a. 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" (2021) guidance and part 5 of 'Keeping children safe in education' 2021.
- Timothy Hackworth Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
  - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our Safeguarding Policy.

- Timothy Hackworth Primary School recognises 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.
- Timothy Hackworth Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Timothy Hackworth Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our Safeguarding 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 support.
    - Implement appropriate sanctions in accordance with our Behaviour (Respectful Relationships) 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.

v Youth Produced Sexual Imagery ("Nudes")

- Timothy Hackworth Primary School recognises that youth produced sexual imagery (known as "nudes") is a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- This section only applies to young people under the age of 18 creating/sharing/receiving nudes of a young person. 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 young person – 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, (Appendix 6), of our school's Safeguarding Policy.
- Timothy Hackworth Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods as part of our PSHE curriculum.
- 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.

b. Online Child Sexual Abuse and Exploitation

- Timothy Hackworth 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.
- Timothy Hackworth Primary School recognises online child sexual abuse and exploitation, (including criminal exploitation), as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- 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.
- We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community via our school website.
- If we are made aware of an incident involving online child sexual abuse we will:
  - Act in accordance with our Safeguarding Policy 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 and 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 Education Durham or Durham Police.
- If learners at any other setting(s) 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.

c. Indecent Images of Children (IIOC)

- Timothy Hackworth 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 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 Safeguarding 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 we are 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 we are 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 we are 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;
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our Allegations Management procedures;
  - Quarantine any devices until police advice has been sought.

d. 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 our school's Safeguarding Policy.

e. Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Timothy Hackworth Primary School.
- Full details of how we will respond to cyberbullying are set out in our Anti-Bullying Policy.

f. Online Hate

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

g. Online Radicalisation and Extremism

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

11. Useful Links for Educational Settings

Education Durham

Paul Hodgkinson, EDA with responsibility for Online Safety:
03000265841(paul.hodgkinson@durham.gov.uk)

Durham SCB

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

Durham Police:

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

Other:

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

National Links and Resources for Educational Settings

CEOP:
www.thinkuknow.co.uk
www.ceop.police.uk

Childnet: www.childnet.com

Internet Matters: www.internetmatters.org

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

Lucy Faithfull Foundation: www.lucyfaithfull.org

Parent Protect https://www.parentsprotect.co.uk/ - this includes advice for parents on peer-on-peer abuse and how to cope if your child has got into significant trouble online.

NSPCC: www.nspcc.org.uk/onlinesafety

ChildLine: www.childline.org.uk

Net Aware: www.net-aware.org.uk

The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

UK Safer Internet Centre: www.saferinternet.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

360 Safe Self-Review tool for schools: www.360safe.org.uk

Parentzone (Google Internet Legends) https://parentzone.org.uk/

National Links and Resources for Parents and Carers

Internet Matters: www.internetmatters.org

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

Action Fraud: www.actionfraud.police.uk (This is the place to report ransomware, scams etc.)

CEOP:
www.thinkuknow.co.uk
www.ceop.police.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

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

Lucy Faithfull Foundation: www.lucyfaithfull.org

Parent Protect - advice for parents having difficulties e.g. Peer on peer abuse
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