The Grove Primary School

"The Grove School Cares"

Online Safety Policy

December 2018

Ms Bernadette Atkinson, Head Teacher
Oakfield Lane, The Grove, Consett, Co. Durham, DH8 8AP
Tel 01207 502938
Email: thegrove@durhamlearning.net

The Grove Primary School
Online Safety Policy

Document Control

Document reference:	Online Safety Policy	**Date implemented:**	04/09/2018
Version:	18.1	**Date modified:**	05/12/2018
Revision due date:	04/09/2019	**Publication:**	External
Reviewed by:	S Hastings (Covering Subject Lead) C Skinner (Technical) C Walton (Subject Lead)	**Sign and date:**	05/12/2018
Authorised by:	B Atkinson Governing Body	**Sign and date:**	05/12/2018

Change History

Version	Date	Description
17.5	25/05/2018	Reviewed to ensure compliance with Data Protection Act 2018
18.0	01/10/2018	Annual Review and Update
18.1	05/12/2018	Updated references to safeguarding policy

Related Documents/Policies

References	Title
	Data Protection Policy
	EYFS Acceptable Use Policy
	KS1 Acceptable Use Policy
	KS2 Acceptable Use Policy
	Teaching Staff Acceptable Use Policy
	Non teaching staff Acceptable Use Policy
	Staff Managing Official Social Media Acceptable Use Policy
	Social Media Policy
	Digital Images Policy
	Behaviour Policy
	Keeping children safe in school Policy

Contents

Policy Aims

This online safety policy has been written by The Grove 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 as required.

It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2018, Early Years and Foundation Stage 2017 'Working Together to Safeguard Children' 2018 and the Durham LSCB procedures.

The purpose of The Grove Primary School online safety policy is to:

- Safeguard and protect all members of The Grove 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.

The Grove 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.

Policy Scope

The Grove 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.

The Grove Primary School identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

The Grove Primary School has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.

This policy applies to all staff including the governing body, teaching and support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of The Grove Primary School (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

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

Links with other policies

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

- Acceptable Use Policies (AUP)
- Behaviour policy
- Keeping children safe in school policy
- Staff Code of conduct policy
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data Protection
- Digital Images policy
- Searching, screening and confiscation policy
- Social media policy

Monitoring and reviewing the online safety policy

As technology in this area evolves and changes rapidly. The Grove 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 Headteacher and child protection team 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.

Roles and Responsibilities

The Grove Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety. The Headteacher and Governing body have a legal responsibility to safeguard children and staff and this will include online activity.

The Designated Safeguarding Lead (DSL) is Bernadette Atkinson has lead responsibility for online safety.

The school has appointed Phillip Marshall as the member of the Governing Body to take lead Responsibility for online safety.

The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code 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 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.

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.
- 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 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 termly with the governor with a lead responsibility for online safety.

Online Safety Groups/Committees

Here at The Grove Primary School we have established an online safety committee who work together to promote online safety as a whole school, our online safety committee consists of:

- Designated Safeguarding Lead
- Computing Head of Subject
- Technical staff
- Governor member
- SENCO
- Parents/Carers (please note school may not wish parents/carers to always be present due to confidential nature of some issues discussed)
- Pupils/children (please note school may not wish children to always be present due to confidential nature of some issues discussed)
- Other community members (e.g. local Police)

The Online Safety Group will support and deliver the key online safety tasks of the DSL and to promote our online safety ethos as a whole school. The group report regularly to the governing body to help inform them of existing practice and localised concerns.

Key responsibilities of staff

All members of staff play an essential role in creating a safe culture within settings, both on and offline. All members of staff should seek to promote safe and responsible online conduct with and by children as part of the curriculum and as part of their safeguarding responsibilities. All members of staff will need to role model positive behaviours when using technologies, either directly with children or in the wider context. All staff should be aware of and ensure they adhere to the school/setting Acceptable Use Policies (AUPs).

The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies.
- Reading the school Online Safety and Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school/setting systems and data they use and have access to.
- Having an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following school Keeping Children Safe in School Policy and procedures.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Demonstrating an emphasis on positive learning opportunities.
- Taking personal responsibility for professional development in this area.

Additional responsibilities for staff managing the technical environment

Members of staff who are responsible for managing the school technical environment have an essential role to play in establishing and maintain a safe online environment and culture within establishments.

Craig Skinner (IT Network Manager) will be responsible for managing the schools' technical environment and to liaise with any external technical service provider to help ensure that the technical environment within the school is both safe and secure.

In addition to the above, the key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Ensuring that the use of the school network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
- Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users in the Early Years Foundation Stage.

Key responsibilities of children and young people

The essential role and responsibilities for children and young people themselves in relation to their own online safety should not be underestimated. Children are encouraged and empowered to develop safe and responsible online behaviours over time, which will enable them to manage and respond to online risks as they occur.

Children and young people are also more likely to be aware of new developments within technology and may be able to provide schools and settings with an excellent way of keeping up-to-date with the rapidly changing pace of development, especially within social media and the associated apps and games.

The key responsibilities of children and young people are:

- Contributing to the development of online safety policies.
- Reading the school/setting Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

Key responsibilities of parents and carers

Parents /carers play a crucial role in developing children's safe and responsible online behaviours, especially where a majority of children's access will be taking place when they are not on the school site. Schools and settings have a clear responsibility to work in partnership with families to raise awareness of online safety issues. Through this approach, parents/carers can help school to reinforce online safety messages and promote and encourage safe online behaviours wherever, and whenever, children use technology.

The key responsibilities of parents and carers are:

- Reading the school Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the school online safety policies.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

Education and Engagement Approaches

Education and Engagement with Learners

An online safety curriculum will be established and embedded throughout the whole school, to raise awareness and promote safe and responsible internet use amongst learners by:

- Ensuring education about safe and responsible use will precede internet access.
- Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- Online safety education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.
- 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

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 and in accordance with legislation.
- Rewarding positive use of technology in line with the school behaviour policy.
- Implementing appropriate peer education approaches.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Seeking learner voice 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.

Engagement and education of children and young people considered to be vulnerable

- The Grove Primary School recognises that some children may be considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- The Grove Primary School will ensure that differentiated and ability appropriate online safety education is given, with input from specialist staff as appropriate. More information about this can be obtained from our school equality policy or from the SENCO
- When implementing an appropriate online safety policy and curriculum The Grove Primary School will seek input from specialist staff as appropriate, including the SENCO, Child in Care Designated Teacher (Carly Irwin).

Engagement and education of staff

- The online safety policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
- Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- 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 in a variety of ways, on a regular (at least annual) basis. This will be achieved through continuous professional development sessions for all staff and regular updates by bot school staff and external agencies.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- The school will highlight useful online tools which staff should use according to the age and ability of the pupils.

Engagement and education of parents and carers

The Grove 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 will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats.
- This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
- Drawing their attention to the 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, within our home school agreement.
- Requiring them to read our acceptable use policies and discuss the implications with their children.

Reducing online risks

The Grove Primary School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.

- Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer or device.
- The school will audit technology on a termly basis use to establish if the online safety policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the schools leadership team.

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.

Safer Use of Technology

The Grove Primary School uses a variety of online communication and collaboration tools both informally and formally with children, parents/carers and staff. It is therefor important that managers and leaders are aware of this use and provide clear boundaries and expectations for safe use.

Classroom Use

Here at The Grove Primary School we use a wide range of technology within the classroom environment. This includes access to:

- Computers, laptops and tablets
- Internet which may include search engines and educational websites
- Online Learning platform
- Email
- Games consoles and other games-based technologies
- Digital cameras and handheld video cameras
- Action Cameras

All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place. This includes but not limited to;

- Password Protection
- Device Restrictions
- Internet Content Filtering
- Mobile Device Management

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home. The school will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community. We will ensure that the use of internet-derived materials, by staff and learners complies with data protection and copyright laws and acknowledge the source of information.

Supervision of learners will be appropriate to their age 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 learners age and ability.

Key Stage 2

- Learners will use age-appropriate search engines and online tools.
- Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

Managing the school website

Schools are required to publish certain information online – this means that they must have a website. Here at The Grove Primary School our school website is maintained by the IT Network Manager.

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The website will comply with the school's guidelines for publications including accessibility respect for accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- School Email addresses will be published carefully online, using a contact form with CAPTCHA technology to avoid being harvested for spam.
- Pupils work will be published with their permission or that of their parents/carers.
- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The IT Network manager will ensure that editorial access to the school website will remain restricted to only members of staff who have completed the necessary training courses.
- The school will post information about safeguarding, including online safety, on the school website for members of the community.

Publishing images and videos online

Still and moving images and sound add liveliness and interest to a publication, display or website, particularly when children can be included. Nevertheless the security of staff and pupils is paramount. Although common in newspapers, the publishing of children's names with their images is not acceptable by educational settings.

- The school will ensure that all images and videos shared online are used in accordance with the schools digital images policy.
- The school will ensure that all use of images and videos take place in accordance other policies and procedures including Data Protection, Acceptable Use Policies, Codes of Conduct and Social Media policies.
- Inline with the image policy, clear consent/permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

Managing email

Email is an essential method of communication at The Grove Primary School for staff, governors and parents. Un-regulated email can provide routes to the school community that bypass traditional boundaries and therefore use of personal email addresses by staff and governors for any official business is not permitted. Likewise it is the responsibility of all staff and governors to ensure that their use of email at work always complies with data protection legislation and confidential or personal data must not be sent electronically via email unless they are appropriately encrypted.

- All members of staff and governors are provided with a specific school email address to use for any official communication.
- The use of personal email addresses by staff or governors for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- Access to school email systems will always take place in accordance to data protection legislation and in line with other appropriate school policies such as Acceptable use, Data Protection and Confidentiality and Keeping Children Safe in School policies.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.
- Whole -class or group email addresses are assigned to all classes for use with class tablet devices, these may be used for communication outside of the school by only designated members of staff and in accordance with the acceptable use policy for these devices.
- Staff will only use the generic school email address or to communicate with parents/carers by email not their school accounts.
- Excessive social email use can interfere with teaching and learning and will be restricted. Access in school to external personal email accounts may be blocked if deemed necessary by the network manager and or senior leadership team.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The school will have a dedicated system for reporting wellbeing, safeguarding and pastoral issues. This system will be managed by designated and trained staff.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

Official videoconferencing and webcam use for educational purposes

Here at The Grove Primary School any video conferencing will be done using the Skype for Business service and acknowledge that use of webcams for CCTV would require parents to be informed via a privacy notice. Video conferencing introduces exciting dimensions for educational contexts; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet and allow children to explore and source new experiences. The availability of live video can sometimes increase safety — you may believe that you can see who you are talking to — but if inappropriately used; a video link could reveal security details, place staff at risk or be used to exploit and abuse children.

The school acknowledges that videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

- All videoconferencing equipment will be switched off and will be kept securely locked away when not in use when not in use and where appropriate, not set to auto answer.
- 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.
- School videoconferencing equipment will not be taken off school premises without permission from the Network Manager and Head Teacher.
- Staff will ensure that external videoconference opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.

Users

- Pupils will be supervised by a member of staff at all times when using video conferencing technology.
- Parents and carers consent will be obtained prior to children taking part in videoconferencing activities.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only network administrators will be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.
- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site the school will check that they are delivering material that is appropriate for the class.

Appropriate and safe classroom use of the internet and any associated devices

Here at The Grove Primary School we recognise that Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access subject specific curriculum for further information.

- The school/setting's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability.
    - At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
    - At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measures in place.
- All school owned devices will be managed by the Network Manager using only authenticated management software. This includes; RM CC4 Management, Windows Active Directory, Meraki Mobile Device Management. All Equipment will also be filtered using Smoothwall Guardian Proxy Filters.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- The school will ensure that safety features are enabled on adult sites which the staff direct children to use; e.g. Google Safe Search, Restricted Modes.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school/setting requirement across the curriculum.
- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

Management of school learning platforms

Here at The Grove we use Office 365 as our official learning platforms for both our staff and the governing body. The learning platform is to collaborate and share school policies and documentation, lesson planning, resources and also internal school communications.

- Only current members staff and governing body will have access to the learning platform using a school assigned account.
- Senior Leadership team and the Network Manager will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular message and communication tools and publishing facilities.
- Staff will be advised about acceptable conduct and use when using the learning platform.
- All users will be mindful of copyright issues and will only upload appropriate work related content onto the learning platform.
- When staff or governors leave the school or governing body their account or rights to specific school areas will be disabled or transferred to their new establishment if applicable.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
    a) The user will be asked to remove any material deemed to be inappropriate or offensive.
    b) The material will be removed by the site administrator if the user does not comply.
    c) Access to the LP for the user may be suspended.
    d) The user will need to discuss the issues with a member of leadership before reinstatement.
- 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.

Social Media

Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of The Grove 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 Grove Primary School community are expected to engage in social media in a positive, safe and responsible manner.
- All members of The Grove 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 restrict learner and staff access to social media whilst using setting provided devices and systems on site through our web filtering system.
- The use of social media during school hours for personal use is/is not permitted for any students. Staff are permitted to use social media on their own personal devices, which are not connected to the school internet during break and lunch times when not working with children.
- 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 The Grove 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.

Staff personal use of social media

Here at The Grove Primary School all staff are aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. Staff know that they should not be communicating with parents and children on social media and that all commination should come through the schools approved channels. Staff have also been made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the schools 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 The Grove 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 communication between staff and members of the school community on school business will take place via official approved communication channels.
- 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 Headteacher.
- 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 Headteacher.
- Any communication from learners and parents received on personal social media accounts will be reported to the Designated Safeguarding lead at the earliest possible time.

Learners Personal Use of Social Media.

- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the School will actively promote this to all children in school and discourage them from creating accounts using social media, this will be done, not only through computing and SMSC lessons but throughout the school curriculum.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites outside of school, will be raised with parents/carers, particularly when concerning any underage use of social media sites, games or tools.

Official use of social media

Here at The Grove Primary School we believe that the use of social media has many benefits to the school to enrich communication with parents and the local community.
We use school official social media for the following;

1. To quickly share and celebrate children's achievements, successes and school updates.
2. To demonstrate safe and responsible use of social media
3. To encourage the use of 21st Century technology

- The Grove Primary School official social media channels are:
    - Facebook – www.facebook.com/thegroveps
    - Twitter – www.twitter.com/thegroveps
    - YouTube – www.youtube.com/channel/UC4LoWHvgEHxS_QEleck5O2w

- 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 Headteacher and governing body
- The school haver in place a full social media policy and acceptable use policies for staff managing the official social media channels.
- Leadership staff 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.
- All staff managing official social media channels have read and signed the staff managing social media acceptable use policy.
- Only setting provided email addresses are used to 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, digital images, 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.
- More information about how we use Social Media here at The Grove Primary School can be found in the social media policy on our school website.

Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Sign our social media acceptable use policy.
    - Always be professional and aware they are an ambassador for the setting.
    - Disclose their official role *and/or* 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 their line manager, the DSL (or deputy) and/or the headteacher any concerns, such as criticism, inappropriate content or contact from learners.

Use of Personal Devices and Mobile Phones

Mobile phones and other personal devices such as tablets, smart watches, e-readers, electronic dictionaries, digital cameras and laptops are considered to be an everyday item in today's society and even children in early years settings may own and use online personal devices regularly at home. Here at The Grove Primary school we actively promote the use of 21st century technology in a safe and controlled environment. We have a number of devices in school such as cameras, laptops and tablet devices which can be used by both staff and children however we ensure that these devices have to correct restrictions and safeguarding settings implemented for safe and correct use by all.

Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all of The Grove Primary School community to take steps to ensure that mobile phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices by young people and adults will be decided by the school and is covered in appropriate policies including the school Acceptable Use policies.
- The Grove 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 the schools.

Expectations for safe use of personal devices and mobile phones*:*

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies such as acceptable use policy, behaviour, child protection, trips and residential visits policy and teaching and learning policy.
- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- All members of The Grove 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 certain areas within the school such as changing rooms, toilets and swimming pools.
- Members of staff will be issued with a work phone number and email address where contact with parents/carers is required.
- Staff will ensure that all school mobile phones and devices must always be used in accordance with the Acceptable Use Policy and any other relevant policies.
- 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 policy.
- All members of The Grove 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 or child protection policies.

Pupils use of personal devices and mobile phones

Here at The Grove Primary school pupils are not allowed to bring personal devices including mobile phones into school under any circumstances. If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.

Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with the head teacher.
- Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. confidentiality, data security, Acceptable Use etc.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school policy then disciplinary action will be taken.
- 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 then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school allegations management policy.

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 image use.
- Visitors are not permitted to use personal devices or mobile phones at any times whilst working with children on the school premises.
- Visitors such as student teachers, volunteers will be given information about the safe and appropriate use of personal devices and mobile phones whilst on school premises and will have to read and sign the student teachers and volunteers acceptable use policy as before working with children.
- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- Under no circumstances can cameras on personal devices or mobile phones be used in accordance with the school's digital images policy.

- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

Policy Decisions

Authorising and managing internet access

The Grove Primary school will allocate Internet access to staff and children on the basis of educational need. Before a user is granted internet access they must sign the appropriate Acceptable usage policy, Parents must also countersign all acceptable use policies for children. If a parent requests that their child/ren do not have internet access in school then we will fully respect their wishes however we would highlight the implications on their child's access to education and we may wish to explore why parents have requested this approach.

The school does also have the right to revoke internet access from pupils if the child is subject to a specific sanction as part of the school behaviour policy.

- All staff, pupils and visitors must read and sign the Acceptable Use Policy before using any school computers/ devices.
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to 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.
- When considering access for vulnerable members of the community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private and to promote good practice to children.

Filtering and Monitoring

No filtering or monitoring solution can offer schools and setting 100% protection from exposure to inappropriate or illegal content, so it is equally important that they can demonstrate that they have taken all other reasonable precautions to safeguard children and staff. Such methods we have adapted at here at The Grove Primary School include appropriate modelling and supervision of children when using the internet, requiring children and staff to sign an acceptable Use Policy (AUP), and embedding a robust, up to date and comprehensive online safety curriculum throughout school.

Filtering and Monitoring

- The Grove Primary School governors and senior leadership team have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The governors and senior leadership team 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 along with technical staff 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

- The school's broadband connectivity is provided through Durham County Council ICT School Services.
- We use Smoothwall Filtering which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- Senior Leadership team and the network manager ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
    - Turn off monitor/screen and report the concern immediate to a member of staff in a discreet manner.
    - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and the network manager.
    - 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

- The Grove Primary School will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
    - Physical teacher supervision when children are using devices.

    - Regularly monitoring internet activity through the use of Smoothwall.
    - The headteacher receives daily reports of any suspicious activity.
- If a concern is identified via monitoring approaches the school 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.

Managing Personal Data Online

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

Technical Security

The Grove Primary School IT System is set up and managed to ensure that the school is safeguarding both staff and pupils. The school strives to ensure that all systems and infrastructure meets the online safety technical requirements. Craig Skinner (IT Network Manager) will be responsible for managing the schools' technical environment and to liaise with any external technical service provider including the local authority to help ensure that the technical environment within the school is both safe and secure.

Security and Management of Information Systems

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

- The school will carry out a technical and security audit on a half termly basis.
- The security of the school information systems and users will be reviewed regularly.
- Virus protection is installed on all workstations and devices on site and will be monitored and updated regularly.
- Encryption for personal data sent over the Internet
- Ensuring that no physical data is taken off site where possible (such as via portable media storage)
- Ensuring that where possible all data is stored on the school cloud platforms and accessed via appropriate secure remote access procedures.
- Not using portable media without specific permission of the network manager. All portable media will be restricted from read/write access automatically by the antivirus software.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network and within the cloud storage for will be checked regularly to ensure integrity of the data, system and 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 users in our early years setting.
- All users are expected to log off or lock their screens/devices if systems are unattended.
- All users have an idle timeout setting enforced so computers will lock after a period of inactivity.

Further information about technical environment safety and security can be found in the data protection policy and Acceptable Usage Policies.

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.

- With the exception of children in Early Years, 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.
    - Change their passwords on an annual basis for children and every 180 days for staff.

Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
    - Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Team or Kent Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or deputy head teacher in their absence will speak with Durham Police first to ensure that potential investigations are not compromised.

Concerns about Learners Welfare

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

Staff Misuse

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

Procedures for Responding to Specific Online Incidents or Concerns

Online Sexual Violence and Sexual Harassment between Children

- Our setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2018.
- The Grove 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 Child Protection Policy.
- The Grove Primary School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- The Grove Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- The Grove 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 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 child protection and anti-bullying policies.
    - If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our school 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 ("Sexting")

- The Grove Primary School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- The Grove 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.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
        - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
    - Act in accordance with our child protection policies and the relevant Durham LSCB procedures.
    - Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Store the device securely.
        - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
    - Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed. Additional resources are available on the Extranet for both Pupils and Parents
    - Make a referral to First Contact and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
    - Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
        - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.

- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

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

- The Grove 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.
- The Grove 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).
- 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 on our school website.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our child protection policies and the relevant Durham LSCB procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to First Contact (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child is at immediate risk.
    - Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education 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.

Indecent Images of Children (IIOC)

- The Grove 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 Kent Police and/or the Education Safeguarding Team.
- If made aware of IIOC, we will:
    - Act in accordance with our child protection policy and the relevant Durham LSCB 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 headteacher 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.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at The Grove Primary School
- Full details of how we will respond to cyberbullying are set out in our behaviour policy which can be found on the school website.

Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at The Grove 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 DSL (or deputy) will obtain advice through First Contact or Durham Police

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 through our filtering and monitoring procedures.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

Appendix A

Procedures for Responding to Specific Online Incidents or Concerns

Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

- The Grove Primary School ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting").
- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers. This may include, family or community assemblies, safeguarding lessons or sessions in school, newsletters and information sent to parents, information posted on the school website and or official social media channels.
- The Grove Primary School regards "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead (Bernadette Atkinson)
- The school will follow the guidance as set out in 'Sexting in schools: youth produced sexual imagery and how to handle it'
- If the school are made aware of incident involving creating youth produced sexual imagery the school will:
    - Act in accordance with the schools Keeping Children Safe In School Policy and the relevant LSCB procedures
    - Immediately notify the designated safeguarding lead.
    - Store the device securely.
    - Carry out a risk assessment in relation to the children(s) involved.
    - Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
    - Make a referral to children's social care and/or the police (as needed/appropriate).
    - Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Implement appropriate sanctions in accordance with the schools behaviour policy but taking care not to further traumatise victims where possible.
    - Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
    - Inform parents/carers about the incident and how it is being managed.
- The school will not view any images suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead).
- The school will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the school network or devices then the school will take action to block access to all users and isolate the image.
- The school will take action regarding creating youth produced sexual imagery, regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

Responding to concerns regarding Online Child Sexual Abuse and Exploitation

- The Grove Primary School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- The School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead Bernadette Atkinson.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately from Durham Police.
- If the school are made aware of incident involving online child sexual abuse of a child then the school will:
    - Act in accordance with the schools Keeping Children Safe in School Policy and the relevant LSCB procedures.
    - Immediately notify the designated safeguarding lead.
    - Store any devices involved securely.
    - Immediately inform Durham police via 101 (using 999 if a child is at immediate risk)
    - Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
    - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved.
    - Make a referral to children's social care (if needed/appropriate).
    - Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Inform parents/carers about the incident and how it is being managed.
    - Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.
- The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils at other schools are believed to have been targeted then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.
- The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP report button the school website homepage.

Responding to concerns regarding Indecent Images of Children (IIOC)

- The Grove Primary School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and or Durham Police.
- If the school is made aware of Indecent Images of Children (IIOC) then the school will:
    - Act in accordance with the schools Keeping Children Safe in School policy and the relevant Durham County Council Safeguarding Child Boards procedures.
    - Immediately notify the school Designated Safeguard Lead.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF),Durham police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).
- If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:
    - Ensure that the Designated Safeguard Lead is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
- If the school are made aware that indecent images of children have been found on the school's electronic devices, then the school will:
    - Ensure that the Designated Safeguard Lead is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
    - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
    - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
    - Follow the appropriate school policies regarding conduct.

Responding to concerns regarding radicalisation and extremism online

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the Keeping Children Safe in School policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the Education Safeguarding Team and/or Durham Police.

Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of The Grove Primary School community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately from Durham Police.
- Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.
- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools online safety ethos.
- Sanctions for those involved in online or cyberbullying may include:
    - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils involved in online bullying will be informed.
    - The Police will be contacted if a criminal offence is suspected.

Responding to concerns regarding online hate

- Online hate at The Grove Primary School will not be tolerated. Further details are set out in the schools anti-bullying and behaviour policies.
- All incidents of online hate reported to the school will be recorded.

- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. anti-bullying, behaviour etc.
- The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately from Durham Police.

Appendix B

Permissible Use of Actions

	Staff & Adults					Pupils			
	Allowed	Allowed for selected staff	Allowed when children are not present	Allowed only in the Staff Room	Not Allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not Allowed
Personal Devices can be handed in for secure storage									x
Personal Devices may be carried around the school		x	x						x
Personal Devices may be turned on in school			x						x
Personal Devices may be used in lessons			x						x
Personal Devices may be used in social time	x								x
Cameras may be used on personal devices					x				x
Personal Devices may use the school wireless network					X				x
Devices may be used to access social media				x					x
Use of school systems for personal use (e.g. E-mail, Shopping)					x				x

Appendix C

Acceptable User Actions (Children and Adults)

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Illegal and Unacceptable
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					x
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					x
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					x
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					x
	Pornography				x	
	Promotion of any type of discrimination				x	
	Threatening behaviour				x	
	Promotion of extremism or terrorism				x	
	Using school systems to run a business				x	
	Bypassing filtering systems				x	
	Infringing Copyright				x	
	Revealing or publishing personal data or network access information				x	
	Creating or propagating viruses or harmful files				x	
	Deliberately downloading files to limit internet usage by others				x	

	Online Gaming (Non-Educational)				x	
	Online Gaming (Educational)			x		
	Gambling				x	
	Shopping				x	
	File Sharing				x	
	Access to Social Media		x	x		
	Video Broadcasting e.g. uploading to YouTube			x		
	Use of YouTube (or other video site) (educational)			x		
	Use of YouTube (or other video site) (Non-educational)				x	

Pupil Incidents	Action / Sanction								
	Refer to Class Teacher	Refer to Head	Refer to Police	Refer to Technical Support	Inform Parents	Removal of internet access rights	Confiscate Device and hand to parents	Warning	Further Action
Deliberately trying to access material which could be considered as illegal	x	x	x	x					
Use of a mobile device contrary to the school rules					x		x		x
Use of non-educational sites during lessons				x					
Unauthorised use of Social Media during the school day	x				x	x			
Accessing another pupils account	x							x	
Allowing others to use your own account	x							x	
Attempting to access a staff account		x		x	x	x			x
Sending a text or message which is deliberately hurtful		x			x		x		x
Attempting to damage or destroy the work of others		x		x	x	x			x
Attempting to bypass the filtering system		x		x	x	x			x
Deliberately trying to access offensive or pornographic material		x		x	x	x			x
Deliberately sending or receiving material which is in breach or copyright or data protection laws		x	x	x	x	x			x

Staff Incidents	Action / Sanction								
	Refer to Line Manager	Refer to Head	Refer to Police	Refer to Technical Support	Refer to HR / LADO	Removal of internet access rights	Warning	Suspension	Further Action
Deliberately trying to access material which could be considered as illegal		x	x		x				
Use of a mobile device contrary to the school rules		x					x		
Inappropriate use of Social Media during the school day		x		x		x	x		
Careless misuse of data e.g. accidental use of memory sticks		x		x			x		
Deliberate misuse of data e.g. unauthorised use of cloud based storage systems		x		x				x	
Allowing others to use your own account		x		x			x		
Attempting to access an administrative account without permission		x		x				x	
Sending a text or message that is regarded as offensive, harassment or of a bullying nature		x			x			x	x
Attempting to bypass the filtering system		x		x				x	x
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students / pupils		x			x			x	x
Actions which could compromise the staff member's professional standing and or bring the institution into disrepute		x						x	x
Accidentally accessing offensive or pornographic material without reporting it		x		x			x		
Deliberately trying to access offensive or pornographic material		x	x	x				x	x
Deliberately sending or receiving material which is in breach or copyright or data protection laws		x	x	x				x	x

Appendix D

Questions to support DSLs responding to concerns relating to youth produced sexual imagery

The following statements may DSLs to consider how best to respond to concerns relating to youth produced sexual imagery:

Child/Young person involved

- What is the age of the child(ren) involved?
    - If under 13 then a consultation/referral to Children's Social Care should be considered.
    - If an adult (over 18) is involved then police involvement will be required. Contact 101 or 999 if there is risk of immediate harm.
- Is the child able to understand the implications of taking/sharing sexual imagery?
- Is the school or other agencies aware of any vulnerability for the children(s) involved? E.g. special education needs, emotional needs, children in care, youth offending?
- Are there any other risks or concerns known by the school or other agencies which may influence decisions or judgements about the safety and wellbeing of the child(ren) involved? E.g. family situation, children at risk of sexual exploitation?

Context

- Is there any contextual information to help inform decision making?
    - Is there indication of coercion, threats or blackmail?
    - What was the intent for taking/sharing the imagery? E.g. was it a "joke" or are the children involved in a "relationship"?
        - If so is the relationship age appropriate? For primary schools a referral to social care regarding under age sexual activity is likely to be required.
    - Is this behaviour age appropriate experimentation, natural curiosity or is it possible exploitation?
- How were the school made aware of the concern?
    - Did a child disclose about receiving, sending or sharing imagery themselves or was the concern raised by another pupil or member of the school community? If so then how will the school safeguard the pupil concerned given that this is likely to be distressing to discuss.
- Are there other children/pupils involved?
    - If so, who are they and are there any safeguarding concerns for them?
    - What are their views/perceptions on the issue?
- What apps, services or devices are involved (if appropriate)?
- Is the imagery on a school device or a personal device? Is the device secured?
    - **NB: Schools and settings must NOT print/copy etc. imagery suspected to be indecent – the device should be secured until advice can be obtained.**

The Imagery

- What does the school know about the imagery? (Be aware it is unlikely to be necessary for staff to view the imagery)

  - Is the imagery potentially indecent (illegal) or is it “inappropriate”?
  - Does it contain nudity or sexual acts?
- Does the child(ren) know who has accessed the imagery?
  - Was it sent to a known peer (e.g. boyfriend or girlfriend) or an unknown adult?
- How widely has the imagery been shared? E.g. just to one other child privately, shared online publically or sent to an unknown number of children/adults?

Action

- Does the child need immediate support and or protection?
  - What is the specific impact on the child?
  - What can the school put in place to support them?
- Is the imagery available online?
  - If so, have appropriate reports been made to service providers etc.?
- Are other schools/settings involved?
  - Does the relevant Designated Safeguarding Lead need to be identified and contacted?
- Is this a first incident or has the child(ren) been involved in youth produced sexual imagery concerns before?
  - If so, what action was taken? **NB repeated issues will increase concerns for offending behaviour and vulnerability therefore an appropriate referral will be required.**
- Are the school child protection and Keeping Children Sage In Education and practices being followed?
  - Is a member of the child protection team on hand and is their advice and support available?
- How will the school inform parents?
  - With older pupils it is likely that DSLs will work with the young person to support them to inform parents
- Can the school manage this issue internally or are other agencies required?
  - Issues concerning adults, coercion or blackmail, violent/extreme imagery, repeated concerns, vulnerable pupils or risk of significant harm will always need involvement with other agencies.

Appendix E

Notes on the Legal Framework

Many young people and indeed some staff and adults use the Internet regularly without being aware that some of the activities they take part in are potentially illegal.

This section is designed to inform users of potential legal issues relevant to the use of electronic communications. It must not replace professional advice and schools and settings should always consult with their Area Safeguarding Adviser or the Education Safeguarding Adviser (Online Protection) from the Education Safeguarding Team, Legal representation, Local Authority Designated Officer or Kent Police if they are concerned that an offence may have been committed.

Please note that the law around this area is constantly updating due to the rapidly changing nature of the internet and this list is not exhaustive.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a "higher law" which affects all other laws. Within an education context, human rights for schools and settings to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. Schools and settings are obliged to respect these rights and freedoms, balancing them against rights, duties and obligations, which may arise from other relevant legislation.

Data protection and Computer Misuse

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film, video and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation.

Data Protection Act 2018

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, organisations have to follow a number of set procedures.

The Computer Misuse Act 1990 (sections 1 - 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

The Protection of Freedoms Act 2012

This act requires schools to seek permission from a parent / carer to use Biometric systems.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Obscene and Offensive Content including Hate and Harassment

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence and this includes electronic transmission. For the purposes of the Act an article is deemed to be obscene if its effect is to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the content. This offence can result in imprisonment for up to 5 years.

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This offence can result in imprisonment for up to 2 years.

Protection from Harassment Act 1997

This Act is relevant for incidents that have happened repeatedly (i.e. on more than two occasions). The Protection from Harassment Act 1997 makes it a criminal and civil offence to pursue a course of conduct which causes alarm and distress, which includes the publication of words, which he/she knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

The victim can also bring a civil claim for damages and an injunction against the abuser, although in reality this is a remedy that is only used by individuals with the financial means to litigate, and only possible if the abuser can be identified, which is not always straightforward.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Public Order Act 1986 (sections 17 — 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

The Protection of Freedoms Act 2012 (2A and 4A) and Serious Crimes Act 2015 (section 76) - Stalking and Harassment

The Protection of Freedoms Act 2012 was updated in 2015 and two sections were added regarding online stalking and harassment, section 2A and 4A. Section 2A makes it offence for a perpetrator to pursue a course of conduct (2 or more incidents) described as "stalking behaviour" which amounts to harassment. Stalking behaviours include following, contacting/attempting to contact, publishing statements or material about the victim, monitoring the victim (including online), loitering in a public or private place, interfering with property, watching or spying. The Serious Crime Act 2015 Section 76 also created a new offence of controlling or coercive behaviour in intimate or familial relationships which will include online behaviour.

Criminal Justice and Courts Bill 2015 (section 33) - Revenge Pornography

Section 33 makes it an offence to share private, sexual materials, either photos or videos, of another person without their consent and with the purpose of causing embarrassment or distress, often referred to as "revenge porn". The offence applies both online and offline and to images which are shared electronically or in a more traditional way so includes the uploading of images on the internet, sharing by text and e-mail, or showing someone a physical or electronic image. This offence can result in imprisonment for up to 2 years.

Sending images of this kind may, depending on the circumstances, also be an offence under the Communications Act 2003 or the Malicious Communications Act 1988. Repeated behaviour may be an offence under the Protection from Harassment Act 1997. This law and the term "revenge porn" only applies to images or videos of those aged 18 or over. For more information access: www.revengepornhelpline.org.uk

Libel and Privacy Law

These matters will be dealt with under civil rather than criminal law.

Libel is defined as 'defamation by written or printed words, pictures, or in any form other than by spoken words or gestures' and as such could the author could be held accountable under Defamation law which was created to protect individuals or organisations from unwarranted, mistaken or untruthful attacks on their reputation. Defamation is a civil "common law" tort in respect of which the Defamation Acts of 1952 and 1996 provide certain defences. It applies to any published material that damages the reputation of an individual or an organisation, and it includes material published on the internet.

A civil action for defamation can be brought by an individual or a company, but not by a public authority. Where defamatory material is posted on a website, the person affected can inform the host of its contents and ask the host to remove it. Once the host knows that the material is there and that it may be defamatory, it can no longer

rely on the defence of innocent dissemination in the Defamation Act 1996. This means that the person affected could (if the material has been published in the jurisdiction, i.e. in England and Wales) obtain a court order (an injunction) to require removal of the material, and could sue either the host or the person who posted the material for defamation.

If social media is used to publish private and confidential information (for example breaches of data protection act) about an individual, then this could give rise to a potential privacy claim and it is possible for individuals to seek an injunction and damages.

Education Law

Education and Inspections Act 2006

Section 89 of the states that every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents. This act (89.5) gives headteachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

The Education Act 2011

Section 13 makes it an offence to publish the name of a teacher who is subject to an allegation until such a time as that they are charged with an offence. All members of the community need to be aware of the importance of not publishing named allegations against teachers online as this can lead to prosecution. Schools should contact the LADO team for advice.

Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. This act gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. The DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for head teachers, staff and governing bodies" www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The School Information Regulations 2012

This act requires schools to publish certain information on its website: https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Sexual Offences

Sexual Offences Act 2003

There are many offences under the Sexual Offence Act 2003 which can be related to or involve the misuse of technology. This includes (but is not limited to) the following points.

Section 15 - Meeting a child following sexual grooming. The offence of grooming is committed if someone over 18 has communicated with a child under 16, at least twice (including by phone or using the Internet) and meets

them or travels to meet with them anywhere in the world with the intention of committing a sexual offence. This offence can result in imprisonment for up to 10 years.

Causing or inciting a child under 16 to watch or take part in a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. Any sexual intercourse with a child under the age of 13 commits the offence of rape.

- **Section 8. Causing or inciting a child under 13 to engage in sexual activity** (Can result in imprisonment for up to 14 years)
- **Section 9. Sexual Activity with a child** (Can result in imprisonment for up to 14 years)
- **Section 10. Causing or inciting a child (13 to 16) to engage in sexual activity** (Can result in imprisonment for up to 14 years)
- **Section 11. Engaging in sexual activity in the presence of a child** (Can result in imprisonment for up to 14 years)
- **Section 12. Causing a child to watch a sexual act** (Can result in imprisonment for up to 10 years)
- **Section 13. Child sex offences committed by children (offender is under 18)** (Can result in imprisonment for up to 5 years)

Section 16 - Abuse of position of trust: sexual activity with a child.

It is an offence for a person in a position of trust to engage in sexual activity with any person under 18 with whom they know as a result of being in their professional role. It is also an offence cause or incite a child with whom they are in a position of trust to engage in sexual activity, to engage in sexual activity in the presence of a child with whom they are in a position of trust, or cause a child with whom they are in a position of trust to watch a sexual act. Typically, teachers, social workers, health professionals, connexions staff etc. fall in this category of trust and this can result in imprisonment for up to 5 years.

Indecent Images of Children

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom under two pieces of legislation; **Criminal Justice Act 1988**, section 160 and **Protection of Children Act 1978**, section 1.1.a. Indecent images of children are images of children (under 18 years) depicting sexual posing, performing sexual acts on themselves or others, animals or sadomachisism.

A child for these purposes is considered to be anyone under the age of 18. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This offence can include images taken by and distributed by the child themselves (often referred to as “Sexting”, see section 9.1). Viewing an indecent image of a child on your computer or phone means that you have made a digital image and printing/forwarding/sharing/publishing can be considered to be distribution. A person convicted of such an offence may face up to 10 years in prison.

Criminal Justice and Immigration Act 2008

Section 63 makes it an offence to possess “extreme pornographic images”. 63 (6) identifies that such images must be considered to be “grossly offensive, disgusting or otherwise obscene”. Section 63 (7) includes images of “threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead” must also be “explicit and realistic”. Penalties for possession of extreme pornographic images can be up to 3 years imprisonment.

The Serious Crime Act 2015

Part 5 (Protection of Children) section 67 makes it a criminal offence for an adult (person aged over 18) to send a child (under 16) sexualised communications or sends communications intended to elicit a sexual communications. The offence is committed whether or not the child communicates with the adult. Penalties for sexual communication with a child can be up to 2 years imprisonment.

Section 69 makes it an offence to be in possession of paedophile manuals, information or guides (physically or electronically) which provide advice or guidance on sexually abusing children. Penalties for possession of such content can be up to 3 years imprisonment.

This law also removed references in existing legislation to terms such as child prostitution and child pornography and identified that this should be viewed to be child sexual exploitation.

Appendix F

Online Safety Contacts and References

Durham Support and Guidance

Durham LA Safeguarding team

3rd Floor
County Hall
Durham
County Durham
United Kingdom
DH1 5UJ

03000 265 770

EDA with responsibility for online safety
Paul.Hodgkinson@durham.gov.uk
03000 265841
Pauline.Stewart@durham.gov.uk

Durham Police:
In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Durham Police via 101

Information and advice on CSE
http://www.eraseabuse.org/

Durham Local Safeguarding Children Board (LSCB): http://www.durham-lscb.org.uk/

ICTSS - ICT Support for Durham Schools 03000 261100

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

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

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

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

Kent e–Safety Blog: www.kentesafety.wordpress.com

Lucy Faithfull Foundation: www.lucyfaithfull.org

Know the Net: www.knowthenet.org.uk

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

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Port: www.parentport.org.uk

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

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

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

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

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

Online Compass (Self review tool for other settings): http://www.onlinecompass.org.uk/

Acknowledgements

The Grove Primary School would like to acknowledge the work of Durham County Council and Kent e-Safety strategy group, in producing the policy template.

This edition has been the work of the Kent e-Safety Strategy group and others including (but not limited to) Rebecca Avery, KCC; Mike O'Connell, KCC; Julie Albone, Kent Police, James Blomfield, St. Thomas Catholic School Canterbury; Emma Fruin, Canterbury College; Douglas Hall, Highworth Grammar School for Girls; Natalie Hancock, EiS, KCC; Karl Hopwood, e-Safety LTD; Michelle Hunt, KCC; Adam Page, EiS, KCC; Natalie Saunders, Thurnham Infant School; David Shipley, Kent Police; Tracey Tee, Guston Primary School; Jo Willemse, Great Chart Primary and the Kent Safeguarding Children Board.

The previous editions involved a very wide group of people including (but not limited to) Kent teachers and officers, BECTA, SEGfL (South East Grid for Learning), NAACE and the British Computer Society Expert Schools Panel.

John Allen, KCC; Steve Bacon, NAACE; Mandy Barrow, Heidi Barton, KCC; Peter Banbury, KCC ; Roger Blamire, BECTA; Stephanie Brivio, Libraries; Clive Bonner, EiS, KCC; Martin Carter, Project Salus/SEGfL/Kent Police; Ian Coulson, KCC; Sandra Crapper, Consultant; Les Craggs, KAS; Alan Day, KCC; Janet Davis, KCC; Alastair Fielden, Valence School; Kevin Figg, Westlands; John Fulton, Hartsdown; Maureen Gillham, Weald of Kent Grammar; Keith Gillett, Seal Primary; Michael Headley, EiS, KCC; Greg Hill, SEGfL; Doreen Hunter, Deanwood Primary Technology School; Rachel Keen, SENICT ; Andrew Lamb, Whitfield Primary; Steve Moores, Maidstone Grammar; Steve Murphy, Drapers Mills Primary; Paul Newton, Kent NGfL; Richard Packham, EiS, KCC; Godfrey Pain, Kent Police; Heather Pettitt, SEGfL; Andy Place, KCC; Ian Price, Child Protection; Sandra Patrick, Kent NGfL; Tom Phillips, KCC; Graham Read, Simon Langton Girls Grammar; Judy Revell, KCC; Chris Ridgeway, Invicta Grammar; Martin Smith, Highsted Grammar; Chris Shaw, EiS; Linda Shaw, Kent NGfL; Chris Smith, Hong Kong; John Smith, Wakefield LEA; Helen Smith, KCC; Sharon Sperling, Libraries; Laurie Thomas, Kent; Clare Usher, Hugh Christie; Gita Vyas, Northfleet School for Girls; Ted Wilcox, Borden Grammar. Nick Roberts, Sussex LEA; Graham Stabbs, St Margarets at Cliffe Primary; Brian Tayler, ICT; Marc Turner, EiS, KCC; Joanna Wainwright, KCC; Richard Ward, KCC; Theresa Warford, Libraries; Carol Webb, Invicta Grammar; Pam Wemban, Riverview Junior School; Ian Whyte, Plaxtol Primary; Chris Woodley, KCC; Rebecca Wright, KCC; Ian White, SWGfL.