Lumley Infant and Nursery School

Online Safety Policy

March 2018

Contents

1. Creating an Online Safety Ethos

1.1 Aims and policy scope

Lumley Infant and Nursery School recognises that online safety is an essential element of safeguarding children and adults in the digital world, particularly when using technology such as computers, tablets, mobile phones or games consoles both in and out of school. It includes education for all members of the community on risks and responsibilities and is part of the 'duty of care' that applies to everyone working with children.
'Keeping children safe in education' implemented in September 2016 highlights a range of specific statutory responsibilities for schools regarding online safety which governing bodies need to be aware of. This includes the need for all staff to be aware of the role of technology within sexual and emotional abuse and also Child Sexual Exploitation and radicalisation and the need for all staff to be aware that abuse can be perpetrated by children themselves and specifically identifies sexting and cyberbullying.

The Early Years Foundation Stage framework 2014 highlights that early years settings should ensure that children are taking steps to understand and explore the world around them. This will include the use of technology. Section 3.4 also highlights the need for early years settings to have a safeguarding policy in place regarding the use of mobile phones. Section 3.6 also highlights the need for staff to have appropriate training to recognise child abuse and inappropriate behaviour (including the sharing of images).

+ Lumley Infant and Nursery School identifies that the internet and information communication technologies are an important part of everyday life, therefore 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.
+ Lumley Infant and Nursery 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.

The purpose of Lumley Infant and Nursery School's Online Safety Policy is to:

- Promote the safe and responsible use technology.
- Safeguard and protect all members of Lumley Infant and Nursery School community online.
- To enable all staff to work safely and responsibly, to model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

+ This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.
+ This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.
+ This policy must be read in conjunction with other relevant school policies including safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing, Personal Social and Health Education (PSHE).

1.2 ***Writing and reviewing the online safety policy***

Lumley Infant and Nursery School Online Safety Policy is based on the Durham County Council online safety policy template based on guidance for educational settings issued by Kent County Council.

GUIDANCE FOR EDUCATIONAL SETTINGS

- The policy has been approved and agreed by the Senior Leadership Team and Governing Body.
- The school has appointed Gill Stephenson as the member of the Governing Body to take lead responsibility for online safety.
- The Online Safety Policy and its implementation will be reviewed by the school annually or sooner if required.

The Designated Safeguarding Lead (DSL) is Mrs Tracey Wilson, Head Teacher.

The Online Safety Lead is Mrs Louise Phillips, Deputy Head Teacher.

The Online Safety Lead for the Governing Body is Gill Stephenson.

Policy approved by Head Teacher: Mrs Tracey Wilson.	Date: March 2018
Policy approved by Governing Body: Gill Stephenson [Chair of Governors]	Date: March 2018
Policy Review date:	Date: March 2019

1.3 Key responsibilities for the community

All members of our school community have an essential role to play in ensuring the safety and wellbeing of others, both on and offline. It is important that all members of the community are aware of these roles and responsibilities and also know how to access and seek support and guidance.

1.3.1 The key responsibilities of the school leadership team are:

- To promote online safety to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- To ensure that online safety is viewed by the whole community as a safeguarding issue and proactively develop a robust online safety culture.
- To support the Designated Safeguarding Lead (DSL) and the Online Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensure there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content whilst ensuring children have access to required educational material.
- To work with Durham LA Technical staff in monitoring the safety and security of our school systems and networks and to ensure that the school's network system is actively monitored.
- To ensure all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.

- To ensure that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- To review online safeguarding records and using them to inform and shape future practice.
- To ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- To ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.

1.3.2 Key responsibilities of the Designated Safeguarding Lead (DSL) / Online safety lead

1.3.2 The key responsibilities of the Online Safety Lead are:

- To work with the closely with the DSL [Tracey Wilson, Head Teacher] to help ensure that all safeguarding incidents either online or otherwise are dealt with following the schools safeguarding procedures.
- To coordinate participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- To ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- To work with the school lead for data protection and data security to ensure that practice is in line with current legislation.
- To keep a record of online safety concerns or incidents and actions taken as part of the schools safeguarding procedures.
- To monitor the school's online safety incidents to identify trends and use this data to update the school's response systems.
- To report to the Governing Body and other agencies as appropriate, regarding online safety concerns and local data.
- To review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis annually with stakeholder input.
- To ensure that that online safety is integrated with other appropriate school policies and procedures.
- Meet regularly with the governor with a lead responsibility for online safety.

1.3.3 The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school's systems and data.
- 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 safeguarding policies 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.

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

The responsibility for managing the technical environment is ultimately the responsibility of the Head Teacher and the Governing Body. Lumley Infant and Nursery School use a Durham LA shared engineer to advise, maintain and develop our infrastructure. The responsibility for managing this service is the responsibility of a member of the SLT. Mrs T. Wilson [Head Teacher] will be responsible for managing any external technical service provider to help ensure that the technical environment within the school is both safe and secure.

- 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’s network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
- Report any breaches or concerns to the DSL 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. [See Durham technical audit sheet]

1.3.5 The key responsibilities of children and young people are:

- Contributing to the development of online safety policies.
- Reading the school's Acceptable Use Policies 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.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.6 The key responsibilities of parents and carers are:

- Reading the school's 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 model 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.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

It will be important that managers and leaders are aware of this use and provide clear boundaries and expectations for safe use.

2.1 Managing the school website

- Lumley Infant and Nursery 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's 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 intellectual property rights, privacy policies and copyright.
- The administrator account for the school website will be safeguarded with an appropriately strong password.

2.2 Publishing images and videos online

- Lumley Infant and Nursery School will ensure that all images and videos shared online are used in accordance with the school image use policy.
- Lumley Infant and Nursery School will ensure that all use of images and videos take place in accordance other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct, social media, use of personal devices and mobile phones etc.
- In line with the image policy, written permission from parents or carers will always be obtained before images of pupils are electronically published.

2.3 Managing email

- All members of staff are provided with a specific school email address to use for any official communication.
- The use of personal email addresses by staff for any official school <u>is not permitted</u>.
- The forwarding of any chain messages 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/setting policies e.g. confidentiality.
- 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 may be used for communication outside of the school *with younger children*.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.4 Official videoconferencing and webcam use for educational purposes

- 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 when not in use and where appropriate, not set to auto answer.
- External IP addresses will not be made available to other sites.
- 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 ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised by teaching staff at all times.
- 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 key administrators will be given access to videoconferencing administration areas or remote control pages.

Content

- 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.

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

- 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.
- The Lumley Infant and Nursery School's internet access will be designed to enhance and extend education appropriate to the age 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
    - In 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.
- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- 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.

2.6 Management of school learning gateways

- Senior Leaders 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 LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff leave the school their account or rights to specific school areas will be disabled.
- A visitor may be invited onto the LP by a member of the leadership team. In this instance there may be an agreed focus or a limited time slot.

3. Social Media Policy – to be read in conjunction with our AUP

3.1. Staff use of Social media

- Expectations regarding safe and responsible use of social media will apply to all members of Lumley Infant and Nursery School's community and exist in order to safeguard both the Lumley Infant and Nursery School and the wider community, on and offline. Examples of social media include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.

- All members of Lumley Infant and Nursery School's community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of Lumley Infant and Nursery School's community.
- All members Lumley Infant and Nursery School's community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others
- The use of social networking applications during school hours for personal use **is not** permitted.
- The use of social media during school hours or whilst using school devices may result in disciplinary or legal action and removal of Internet facilities.
- Any concerns regarding the online conduct of any member of Lumley Infant and Nursery School's community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of Lumley Infant and Nursery School's policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2. Staff personal use of social media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school's Acceptable Use Policy.
- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead.
- All communication between staff and members of the school community on school business will take place via official approved communication channels e.g. general school e-mail, landline or school mobile.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Head Teacher.
- Any communication from pupils or parents received on personal social media accounts will be reported to the schools designated safeguarding lead.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.

- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school's policies relating to safeguarding, confidentiality, data protection etc. and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school.
- Members of staff are encouraged not to identify themselves as employees of Lumley Infant and Nursery School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school/setting and also to safeguard the privacy of staff members and the wider community.
- Members of staff will ensure that they do not represent their personal views as that of Lumley Infant and Nursery School on social media.
- Lumley Infant and Nursery School email addresses will not be used for setting up personal social media accounts.

4. Use of Personal Devices and Mobile Phones read in conjunction with our AUP

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. Mobile phones and personal devices can be used to communicate in a variety of ways with texting, cameras, voice recording and internet accesses all common features.

4.1 Rationale regarding personal devices and mobile phones

- The use of mobile phones and other personal devices by young people and adults will be decided by the Lumley Infant and Nursery School and is covered in appropriate policies including the school's Acceptable Use Policy.
- Lumley Infant and Nursery School recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within school.

4.2 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 the Lumley Infant and Nursery School's Acceptable Use 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.
- Mobile phones and personal devices are not permitted to be used during teaching sessions.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline policy.
- Members of staff will use the school landline, school mobile phone or general email address where contact with pupils or parents/carers is required.
- All members of Lumley Infant and Nursery School's community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of Lumley Infant and Nursery School's community will be advised to use passwords or pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of Lumley Infant and Nursery School's community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school policies.
- The school's mobile phone and devices must always be used in accordance with the Acceptable Use Policy.
- The school's mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode or pin and must only be accessed and used by members of staff.

4.3 Pupils use of personal devices and mobile phones

- Pupil's personal mobile phones and personal devices will be prohibited in school.
- If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Leadership Team.

4.5 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 senior leaders.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- 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.

- 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's Acceptable Use Policy then disciplinary action will be taken.

4.6 Visitors use of personal devices and mobile phones – *read in conjunction with our Visitor AUP*

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school's acceptable use policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school's image use policy.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead [Head Teacher, Tracey Wilson] of any breaches of use by visitors.

5. Policy Decisions

5.1. Reducing online risks

- Lumley Infant and Nursery 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's Leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.
- The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. Under the recommendation of Durham LA Smoothwall is currently in place.
- 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/setting computer or device.
- The school will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.

5.2. Internet use throughout the wider school community

- The school will liaise with local organisations (Feeder Schools, Police etc.) to establish a common approach to online safety.
- The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site

5.3 Authorising internet access

- All staff, pupils and visitors will read and sign the Acceptable Use Policy before using any school resources.
- Parents will be informed that pupils will be provided with supervised Internet access that 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.

6. Engagement Approaches

6.1 Engagement and education of children and young people

- An online safety curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
- Education about safe and responsible use will precede internet access.
- Pupils will be supported in reading and understanding the Acceptable Use Policy in a way that is appropriate to their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Online safety will be included in the PSHE and Computing programmes of study, covering both safe school and home use.

Useful online safety programmes include:

- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- Digital Literacy Scheme of Work: www.digital-literacy.org.uk
- Internet Matters: www.internetmatters.org
- BBC
    - www.bbc.co.uk/webwise
    - www.bbc.co.uk/cbbc/topics/stay-safe
    - www.bbc.co.uk/education

Other suggested links and resources to use with children from Early Years to Sixth form/college provision can be found at: http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials

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

- Lumley Infant and Nursery School is aware that some children may be considered to be more vulnerable online due to a range of factors.
- Lumley Infant and Nursery School will ensure that differentiated and ability appropriate online safety education is given, with input from specialist staff as appropriate (e.g. SENCO, Looked after Child Coordinator).

6.3 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. Discretion and professional conduct is essential when using school 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.
- 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.

6.4 Engagement and education of parents and carers

- Lumley Infant and Nursery School recognise that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school online safety policy and expectations in newsletters, letters, school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.

7. Technical Security

7.1 Managing Personal Data – read in conjunction with our Data Protection Policy

7.2 Security and Management of Information Systems

The responsibility for managing the technical environment is ultimately the responsibility of the Head Teacher and the Governing Body. Lumley Infant & Nursery School employ a LA Shared engineer or service provider to maintain and develop their infrastructure. The responsibility for managing this service rests with the school and should be the responsibility of a member of the SLT.

- The school will complete a technical audit (see attached example on the Extranet) on a termly basis.
- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.

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.

7.3 Filtering and Monitoring

- The governors will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children's exposure to online risks.
- The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
- All monitoring of school systems will take place to safeguard members of the community.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- The school uses educational filtered secure broadband connectivity through Smoothwall and will block all sites on the Internet Watch Foundation (IWF) list.
- Smoothwall blocks sites that fall into categories such as pornography, racial hatred, extremism, etc. Smoothwall produces instantaneous alerts to notifiy the nominated persons of a Safeguarding breach and also generates a weekly notification report to highlight searches. The school has a clear procedure for reporting breaches of filtering which all members of the school community will be made aware of.
- If staff or pupils discover unsuitable sites, the URL will be reported to the Head Teacher or in her absence the Deputy Head and will then be recorded and escalated as appropriate.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
- All changes to the school filtering policy will be logged and recorded.
- The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate by checking notifications highlighted by Smoothwall. A simple log will be kept showing when checks were completed.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Durham Police or CEOP immediately.

7.4 Management of applications (apps) used to record children's progress

- Any use of cloud based systems will follow the guidance from the ICO [Information Commissioner's Office].
- The Head Teacher is ultimately responsible for the security of any data or images held of children.
- Systems which store personal data will be risk assessed prior to use.
- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.
- Parents will be informed of the school's expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

8. Responding to Online Incidents and Safeguarding Concerns

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- All members of the school community will be informed about the procedure for reporting online safety concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
- The Designated Safeguarding Lead (DSL) will be informed of any online safety incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with LSCB systems.
- If there is a possibility that an offence has occurred, then any equipment used should be isolated and left unused to preserve any evidence on the device.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure
- Any complaint about staff misuse will be referred to the Head Teacher
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Pupils, parents and staff will be informed of the school's complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety incidents in accordance with the school behaviour policy where appropriate.

- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact Durham Police via their local station and their EDP.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Durham Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- Parents and children will need to work in partnership with the school to resolve issues.

9. Procedures for Responding to Specific Online Incidents or Concerns

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

+ Lumley Infant and Nursery School will 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. See links at the end of this document
+ Lumley Infant and Nursery School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead, Mrs Tracey Wilson.
+ 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 school's child protection and safeguarding 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 an 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/settings 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/setting 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.

9.2. Responding to concerns regarding Online Child Sexual Abuse and Exploitation

- Lumley Infant and Nursery 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.
- Lumley Infant and Nursery 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 (*Mrs Tracey Wilson*).
- 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 school's child protection and safeguarding 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 (including carrying out relevant checks with other agencies).
    - 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.

9.3. Responding to concerns regarding Indecent Images of Children (IIOC)

- Lumley Infant and Nursery 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/setting 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 Durham LA Education Safeguarding Team.

9.4. 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. Smoothwall filtering is in place. An instantaneous alert notifies the nominated persons of a Safeguarding breach.
- 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 safeguarding 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 Durham LA Education Safeguarding Team and / or Durham Police.

9.5. *Responding to concerns regarding cyberbullying*

- Cyberbullying, along with all other forms of bullying, of any member of Lumley Infant and Nursery School community will not be toleratedAll 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 school's online safety ethos.

9.6. *Responding to concerns regarding online hate*

- Online hate at Lumley Infant and Nursery School will not be tolerated.
- 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 A

Permissible Use

	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
Devices can be handed in for secure storage		X							X
Devices may be carried around the school		X						X	
Devices may be turned on in school		X						X	
Devices may be used in lessons					X			X	
Devices may be used in social time				X				X	
Cameras may be used on devices					X			X	
Devices may use the school wireless network					X			X	
Devices may be used to access social media									X
Use of school systems for personal use (e.g. E-mail, Shopping)					X				X

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	
	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 / Tutor	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						
Use of a mobile device contrary to the school rules		X			X		X	X	
Use of non-educational sites during lessons		X						X	
Unauthorised use of Social Media during the school day		X			X	X		X	
Accessing another pupils account		X			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	
Attempting to bypass the filtering system		X		X	X	X		X	
Deliberately trying to access offensive or pornographic material		X			X	X			
Deliberately sending or receiving material which is in breach or copyright or data protection laws		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					X		
Inappropriate use of Social Media during the school day		X				X	X		
Careless misuse of data e.g. accidental use of non-encrypted memory sticks		X		X			X		
Deliberate misuse of data e.g. unauthorised use of cloud based storage systems		X		X		X	X	X	
Allowing others to use your own account	X	X							
Attempting to access an administrative account without permission		X				X			
Sending a text or message that that is regarded as offensive, harassment or of a bullying nature		X	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	X
Actions which could compromise the staff member's professional standing and or bring the institution into disrepute		X					X	X	X
Accidentally accessing offensive or pornographic material without reporting it		X				X	X	X	
Deliberately trying to access offensive or pornographic material		X	X					X	X
Deliberately sending or receiving material which is in breach or copyright or data protection laws		X				X	X	X	

Appendix B

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?
- Has the child(ren) involved been considered under KSCB 2.2.2 "children who display harmful behaviours" or the KSCB CSE toolkit?

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 safeguarding policies 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 C

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 1998

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 D

Online Safety Contacts and References

Durham Support and Guidance

Durham LA Safeguarding team

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

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/

Links for staff personal use of social media

www.childnet.com/teachers-and-professionals/for-you-as-a-professional
www.childnet.com/teachers-and-professionals/for-you-as-a-professional/professional-reputation
www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/professional-reputation
www.saferinternet.org.uk/about/helpline/faqs

Links relating to online hate crime

www.report-it.org.uk – Report hate crimes
www.stoponlineabuse.org.uk - Report online Sexism, homophobia, biphobia and transphobia
www.homeoffice.gov.uk/crime-victims/reducing-crime/hate-crime/
www.stophateuk.org
www.voiceuk.org.uk
www.victimsupport.org.uk
www.stonewall.org.uk

Acknowledgements

This edition has been the work of the Kent e-Safety Strategy group.