



SCHOOL POLICY

eSafety Policy



Policy Revision Date	16 th July 2019
Review Frequency	Annual
Role / Author	SBM/IT Curriculum Manager
Governing Body Committee/HT	Curriculum & Standards (to be Resources in future)
Date of GB Meeting/HT review for approval	7 th October 2019
Due with Clerk to Governors (where applicable)	20 th September 2019
Governing Body/HT Approval Date	7 th October 2019
Status (draft / approved)	Approved
Date Policy Due for next review:	July 2020

Note:

Please ensure tracked changes are used to highlight changes from the last approved version. The document status should be 'Draft'.

Once the changes have been approved by the Governing Body, the tracked changes can be accepted and the document status changed to 'Approved'.



Policy Review

The following list must be completed prior to submission to the relevant Governing Body meeting/HT for approval.

Links with other Policies	Child Protection Policy, Safeguarding Policy, Anti-Bullying Policy, Home School Agreement, Behaviour Policy, Management of Allegations against Staff, Staff Disciplinary procedures, Student Acceptable Use Agreement, Staff Acceptable Use of IT Policy and Agreement, School Social Media Policy
Model or Locally Produced	Based on HCC Model Policy which has been localised
Are changes to model policy or previous policy clearly identified (e.g. track changes)	Yes
In the view of the HT is the policy related to High, Medium or Low Risk activity to the school	Medium Risk???? Do not have any parameters to measure against – how are we measuring risk?
What are the likely consequences to school of non-compliance	Failure to implement rigorous online safeguarding measures could lead to increased incidences of access to inappropriate content. Potential harm to pupils Potential reputational risk
Are the governors/SLT accountabilities clearly identified	Yes
Are other accountabilities clearly identified	Yes
Are there any particular issues/risks associated with implementation/operation of policy	Lack of effective communication with staff – needs to be regular updates to staff about their responsibilities. Risk is inconsistent approach to online safety and monitoring of pupils’ activity online. Lack of effective communication with pupils and parents about online safety. Not keeping up-to-date with latest legislation and trends regarding online safety means we may not be aware of the latest risks to pupils’ online safety
How will policy effectiveness be evaluated	e-Safety Committee to be formed, chaired by a member of the Governing Body. Review after the report of any incidents
How will HT report to governors on effectiveness and when	Headteacher will regularly update the e-Safety Committee in regards to training, identified risks and any incidents.
When will the policy next be due for renewal (for statutory compliance)	Annually, next review due July 2020
Does the policy impact on available resources	No



1. Introduction

This e-Safety Policy is important to Elson Junior School for a number of reasons, including:

- To ensure there is a clear and consistent approach responding to incidents.
- To ensure that every person responsible for the children is fully aware of his/her responsibilities.
- To set guidelines for the use of IT equipment, used in the school.
- To provide guidelines for using services such as social networking (e.g. blogging, Twitter).

2. Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

- **Users** - refers to staff, members of the governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.
- **Parents** – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.
- **School** – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.
- **Wider school community** – students, all staff, governing body and parents.

Our priority at Elson Junior School is to ensure our school is a safe place for our children, staff and all members of the school community. At Elson Junior School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety, is an area that is constantly evolving and as such, this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is:

- To meet the requirement to equip children and young people to stay safe online, both in school and outside; by supporting them to develop their own understanding of the risks and learning how to keep themselves and others safe online.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeable harm to the student or liability to the school.
- To ensure we respond consistently to protect children and learners, while still enabling them to take age-appropriate and reasonable risks as part of their development.

This policy is available for anybody to read on the Elson Junior School website.

Upon review, all members of staff will sign as read and understood the e-safety policy, the **Staff Acceptable Use Policy, and the School Social Media Policy.**

A copy of the e-safety policy and the Student Acceptable Use Agreement will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.



3. Roles and Responsibilities

3.1 Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:
 - Keep up to date with emerging risks and threats through technology use.
 - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
 - Chair the e-Safety Committee

3.2 Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety Officer, as indicated below.

The Headteacher will ensure that:

- e-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

3.3 e-Safety Officer

The day-to-day duty of e-Safety Officer is devolved to the Assistant Headteacher with responsibility for curriculum.

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology
- Familiarise him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher and governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.

3.4 School Business Manager, liaising with IT Network Support Provider

Staff managing the technical environment have an essential role to play in establishing and maintaining a safe online environment. Staff with technical responsibility should:

- Work closely with the school leaders, designated safeguarding lead as well as pastoral and curriculum staff (where appropriate) to provide expertise relating to appropriate education use of ICT systems and also to ensure that learning opportunities are not unnecessarily restricted by technical safety measures.
- Be clear about procedures they must follow if they discover, or suspect, online safety incidents through monitoring of network activity and the need for these issues to be escalated immediately to the DSL and/or Headteacher in line with existing school safeguarding policies.



- Ensure that an external service provider upholds the online safety practices including referring any concerns to the online safety coordinator or leadership team.
- Ensure that the school network is monitored and any concerns reported to the DSL/Headteacher
- Develop an understanding of the relevant legislation
- Ensure that the school's ICT infrastructure is secure but not so secure that it gets in the way of learning
- Ensure that appropriate anti-virus software and system updates are installed and maintained on all electronic devices

3.5 All Staff

All staff are responsible for safeguarding children on and off line. Their key responsibilities are:

- Contributing to the development of online safety policies
- Reading and adhering to Acceptable Use Policies (AUPs)
- Taking responsibility for the security of school/setting systems and data
- Having an awareness of a range of different online safety and how they relate to safeguarding children. This should include sexting and cyberbullying.
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in curriculum delivery wherever possible
- Staff are responsible for ensuring that children do not use laptops unless supervised by an adult that can monitor their activity
- 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
- Maintain a professional level of conduct in their personal use of technology, both on and off site
- Taking personal responsibility for professional development in this area.

3.6 All Students

Students should take responsibility and take ownership of any online safety policy. They should:

- Contribute to the development of these policies
- Read the Student Acceptable Use Agreement and adhere to it
- Respect the feelings and rights of others both online and offline
- Seek help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues
- Take responsibility for keeping themselves and others safe online
- Take responsibility for understanding risks posed by new technologies
- Assess the personal risk of using any particular technology and behave safely and responsibly to limit those risks.

3.7 Parents and Carers

Parents and carers should:

- Read the Student Acceptable Use Agreement, encourage themselves and their children to adhere to it
- Discuss 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
- Identify changes in behaviour that could indicate that their child is at risk of harm online
- Seek help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

3.8 e-Safety Committee (within the Curriculum committee)

Chaired by the Governor responsible for e-Safety, the e-safety Committee is responsible:



- to advise on changes to the e-safety policy.
- to establish the effectiveness of e-safety training and awareness in the school.
- to recommend further initiatives for e-safety training and awareness at the school.

Established from volunteer students, parents, e-Safety Officer, responsible governor and others, as required, the e-Safety Committee will meet on a half-termly basis.

3.9 Staying safe when using Online Communication

Website

The school will request written permission from parents and carers before images/videos of students are posted online. Images will only be posted in consideration of other safeguarding and data protection policies.

E-mail

Personal emails are not used in the school. A school email address must be used for all communications in a professional context. Staff should be aware that school emails are not private and can be monitored. The risk of sharing data via school email should also be considered. There should be a consideration of the confidentiality of the data as well as a work life balance – staff should not send emails out of working hours unless essential. School staff must 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 it is encrypted. Staff should be appropriately trained and should ensure members of staff use appropriately secure email systems to share any sensitive or personal information.

Classroom use of the Internet

Staff must be aware that no search engine or filtering tool is ever completely safe, and appropriate supervision, use of safe search tools, pre checks of search terms, age appropriate education for pupils and robust classroom management must be in place. However, there is still a risk that children will be exposed to inappropriate content. The quality of information on the internet is variable. Staff and students need to be made aware of how they can critically evaluate the information available. Children are not permitted to bring their own devices into school.

Social Media

There are significant benefits for communication, engagement collaboration and learning via the internet and social media however, alongside this, there are risks associated with users such as staff, pupils and the wider school community. There are many tools that can be used to communicate online with applications like Facebook, Instagram and Snapchat, as well as numerous apps published on a daily basis. These sites are at risk of being exposed to a great deal of advertising and could provide access to inappropriate content. Pupils should be encouraged to limit the amount of personal information they upload and some of the risks of sharing this information.

Staff personal use of social media

'Keeping Children Safe in Education' 2016 highlights that Governing Bodies need to ensure that their settings have "...a staff behaviour policy (sometimes called the code of conduct) which should, amongst other things, include – acceptable use of technologies, staff/pupil relationships and communications including the use of social media". It is therefore essential that schools ensure all members of staff are aware of professional boundaries regarding both their 'on' and 'offline' communication.

Schools cannot ban staff from using social media, but they should offer advice and guidance to ensure that staff remain safe and maintain the necessary professional boundaries. All staff need to be aware:

- Of the importance of considering the material they might publish online so that it doesn't undermine the professional reputation of themselves or their schools, which could result in a disciplinary issue
- That they should use the highest privacy setting when social networking
- Not engage in communication with present or past pupils or parents of these pupils, unless there is a justifiable professional reason.



If it is seen as beneficial for staff to communicate with pupils, this should be set up through an official establishment social networking page, including members of the Senior Leadership Team. These need to provide clear areas of transparency. If there are any pre-existing relationships, these should be declared to the DSL to formally acknowledge the relationship.

The following links may be helpful:

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/advice-and-resources/teachers-and-professionals/professional-reputation
www.saferinternet.org.uk/about/helpline/faqs

Pupils use of social media

The school has a responsibility to ensure that pupils in the school have been provided appropriate education around the safe use of the internet and social media. This is part of the Computing programme of study, but should also be part of the PSHE curriculum.

Many sites have a restriction age of 13. It is not illegal for pupils under this age to access these sites, its just not recommended because of the risk of them being targeted with unsuitable advertisements. If children are using social media sites inappropriately (such as cyberbullying, posting personal information, adding strangers as friends, etc) or there are other safeguarding concerns due to vulnerabilities, etc. then the school should respond to the concern in line with existing policies, e.g. anti-bullying, children protection/safeguarding or behaviour policy. If a child is risk of significant harm then the DSL must be informed and the existing child protection procedures should be followed.

Use of Personal Devices and Mobile Phones

As with many forms of technology, mobile phones and personal devices are undergoing constant development with increased functionality. They are multifunctional tools that are becoming essential in personal and work life. However they can present problems such as:

- Items that can be stolen and damaged
- Used for bullying
- Internet access that can bypass school monitoring and filtering
- Undermine class discipline
- Breach data protection and confidentiality policies
- The use of images to bully

In the context of mobile phones, schools should ensure that:

- Teaching, learning and behaviour should not be impeded
- Staff should be given clear boundaries on professional use and expectations
- Learners should be given explicit education regarding appropriate use of mobile phones and personal devices

Headteachers and Governing Bodies should consider the risk to data protection if they allow staff to use their personal devices for their professional role. Strategies must be implemented to safeguard this data, including:

- Use of passwords
- Data encryption
- Awareness around data protection
- Awareness of Acceptable Use Policies

Any use of mobile or handheld devices should be risk assessed with the involvement of all stakeholders including parents and pupils.

Pupils use of personal devices and mobile phones



The school do not permit pupils to use their mobile phones and personal devices whilst on school premises. If pupils bring these devices to school, they should take the devices to the school office before registration to deposit them. Please ensure that the device is turned off. Devices can then be collected from the school office at the end of the school day.

Staff use of personal devices and mobile phones

The school permits appropriate and proportional staff use of devices in school however, the following guidelines must be adhered to:

- Staff should not use their personal devices for recording images and video
- Bluetooth or other forms of communication should be 'hidden' or switched off during lesson times
- Personal mobile phones or devices should not be used during teaching periods unless permission has been given by a member of the Senior 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's allegations management policy.

3.10 Engagement Approaches

Engagement and education of children and young people

Online safety forms an important part of the Computing curriculum programmes of study for children within schools and this highlights the importance for children to use technology safely and respectfully, understand how to keep personal information private and be able to identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies from an increasingly early age. Children need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Critical awareness of the dangers and consequences of plagiarism, copyright, piracy, reliability and bias will need to be explored. Children will need to develop an understanding on how to become safe and responsible online or digital citizens and this should be developed within an appropriate Personal Social and Health Education (PSHE) curriculum.

Whilst the Computing Curriculum will form an essential part of online safety education for children and young people, safe and responsible use of technologies must be embedded throughout the whole school curriculum to ensure children develop the required range of digital literacy and safety skills as well as to develop online resilience to enable them to become safe and responsible internet users. Keeping children safe in education has highlighted that governing bodies need to "... ensure that children are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum which may include covering relevant issues through personal, social, health and economic education (PSHE) and through sex and relationship education (SRE)" (Section 68).

It is therefore essential that educational settings give consideration as to the most appropriate place within the curriculum for teaching online safety (e-Safety). Whilst this could be part of the computing curriculum or a special event or assembly, best practice is where schools develop and implement a whole school and progressive curriculum which allows pupils to develop over time, appropriate strategies to respond to risk. Online safety education must also be reinforced whenever pupils are using the internet, therefore a computing online approach will not be sufficiently robust.

Useful online safety (e-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

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

Vulnerable children are more likely to take risks in real life as well as online, therefore there needs to be careful consideration around the support and education provided to these pupils, their teachers and carers.

Engagement and education of staff

Online safety education should be part of the annual safeguarding training that statutorily takes place in all schools.

Engagement and education of parents and carers

Technology is a tool that is commonly used in the home environment. It is therefore important that parents and carers are provided with the opportunity to hear about the benefits and risks of technology and how these can be managed.

Awareness-raising with families should focus on:

- The range of different ways children and young people use and access technology e.g. mobile phones, games consoles, tablets and apps etc. not just laptops and computers
- The many positive uses of technology as otherwise online safety can easily become frightening and scaremongering so be aware that the vast majority of interactions and experiences on the internet are positive
- The importance of developing risk awareness and risk management by children and young people (according to their age and ability) and resources parents/carers can use to help discuss online safety.

Management Information Systems

Managing personal data online, schools need to adhere to the data protection act (DPA) and GDPR. It has become a great deal easier to have access to data, therefore providing a greater risk for the misuse of data. The following link to the Information Commissioners Office provides information and teaching resources to support schools in understanding the rules and regulations that sit around data protection <https://ico.org.uk/for-organisations/education/>

Security and Management of Information Systems

Security of school networks is an extremely important issue. The following should be considered:

Local Area Network (LAN) security issues include:

Users must act reasonably e.g the downloading of large files during the working day will affect the service that others receive.

- Users must take responsibility for their network use. For HCC staff, flouting electronic use policy is regarded as a reason for dismissal
- Workstations should be secured against user mistakes and deliberate actions
- Servers must be located securely and physical access restricted
- Virus protection for the whole network must be installed and current
- The server operating system must be secured and kept up to date
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption

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.
- We require staff to use STRONG passwords for access into our system i.e. to include upper case, lower case, numeric and symbols.
- We require staff to change their passwords every 90 days.

Filtering and Monitoring

No filtering or monitoring solution can offer schools and settings 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 may include appropriate supervision, requiring children and staff to sign an Acceptable Use Policy (AUP), a robust and embedded online safety curriculum and appropriate and up-to-date staff training etc. It is vital for all Governing bodies and members of staff to recognise that even with the most expensive and up-to-date security systems and filtering, children or staff can potentially bypass them either via using proxy sites or by using their own devices, which would not be subject to school filtering. Appropriate supervision, policy and procedures and up-to-date education and training are essential. A reliance on filtering and monitoring alone to safeguard children online could lead to a feeling of complacency which may put children and adults at risk of significant harm.

3.11 Procedures for Responding to Specific Online Incidents or Concerns

Responding to concerns regarding Youth Produced Sexual Imagery or “Sexting”

Youth Produced Sexual Imagery or “Sexting” can be defined as images or videos generated by children under the age of 18 that are of a sexual nature or are considered to be indecent. These images may be shared between children and young people and/or adults via a mobile phone, webcam, handheld device or website. Children and young people will always look to push the boundaries, especially when they go through puberty and are an age where they are more sexually and socially aware. Children typically do not use the term ‘sexting’, usually referring to images as ‘selfies’ and may decide to send such pictures or videos for many reasons. For younger children, indecent images or videos may be taken or shared out of curiosity or naivety and for older children, indecent images may be taken or shared as a response to peer pressure, cyberbullying, sexual exploration, impulsive behaviour or even exploitation due to blackmail from a friend, partner or other on or offline contact. There can also be emotional and reputation damage that can come from having intimate photos forwarded to others or shared online, including isolation, bullying, low self-esteem, loss of control, creative of a negative “digital footprint” or online reputation, harassment, mental health difficulties, self-harm, suicide and increased risk of child sexual exploitation.

Whilst it is important for professionals not to condone the creation of youth produced sexual imagery, it is important for professional to recognise that many young people view sharing sexual images as part of a “normal” relationship in today’s modern society. It is important to be aware that young people involved in sharing sexual videos and pictures may be committing a criminal offence. Under Section 1 of the Protection of Children Act 1978 and Section 160 of the Criminal Justice Act 1988 it is a crime to take an indecent photograph or allow an indecent photograph to be taken, make an indecent photograph (this includes downloading or opening an image that has been sent via email); distribute or show an indecent image, advertise indecent images and possess an indecent image or possess an indecent image with the intention of distribution. This applies even if the images are sent or shared by someone under the age of 18, with consent. “Sexts” may be viewed as police evidence and it is essential that schools secure devices and seek advice immediately when dealing with concerns.

The current Association of Chief Police Officers’ (ACPO) position is that...”ACPO does not support the prosecution or criminalisation of children for taking indecent images of themselves and sharing them. Being prosecuted through the criminal justice system is likely to be upsetting and distressing for children, especially if they are convicted and punished. The label of sex offender that would be applied to a child or young person convicted of such offences is regrettable, unjust and clearly detrimental to their future health and wellbeing”.

www.ceop.police.uk/Documents/ceopdocs/externaldocs/ACPO_Lead_position_on_Self_Taken_Images.pdf.



It should be noted that prosecution of children for sharing indecent images for a first offence is rare. The decision to criminalise children and young people for sending sexualised images will need to be considered and made on a case by case basis based on a number of factors including age, intent and vulnerability of children involved.

'Keeping Children Safe in Education' 2016 highlights the need for all members of staff to be aware that abuse can be perpetrated by children themselves, including sexting, and there is a need for all members of staff to be aware of concerning behaviour and appropriate safeguarding responses. It is essential that schools handle 'sexting' incidents as carefully as possible and offer support to all parties involved whilst abiding by the law and also do not compromise police investigations. Should an incident arise which necessitates criminal investigation then it may require the seizure of the phone/device and any other devices involved or identified as potentially having access to the imagery. Schools should ensure the existing policies regarding seizing and searching are robust and up-to-date.

Responding to concerns regarding Online Child Sexual Abuse and Exploitation

Online child sexual abuse within this policy context is specifically defined as when children are sexually abused or exploited via the use of technology and the internet. Typically this is referred to as "online grooming" however this term can sometimes be considered too narrow when considering online child sexual abuse as using the term "grooming" may imply that the behaviour has taken place over a period of time whilst an offender has built a relationship and gained the trust of the victim. Whilst this longer term process still occurs, current trends, identified national (CEOP/NCA) and locally would suggest that the period of engagement between offender and victim can in many cases be extremely brief. In 2015, CEOP identified that the objectives of online child sexual abuse have evolved and can lead to a range of offending outcomes, such as deceiving children into producing indecent images of themselves or engaging in sexual chat or sexual activity over webcam. Online child sexual abuse can also result in offline offending such as meetings between an adult and a child for sexual purposes following online engagement.

Responding to concerns regarding Indecent Images of Children (IIOC)

Schools must be aware of and understand the law regarding indecent images of children. Specifically (but not limited to):

- The Sexual Offences Act 2003 (England and Wales) defines a child, for the purposes of indecent images, as anyone under the age of 18. The Civic Government (Scotland) Act, 1982 replicates this.
- The Sexual Offences Act 2003 (England and Wales) provides a defence for handling potentially criminal images and this is supported by a Memorandum of Understanding which provides guidance on what is and is not acceptable.

It is an offence to possess, distribute, show and make indecent images of children. Making of and distributing indecent images of children includes printing and viewing them on the internet otherwise known as 'downloading'. More information about these offences can be found within the legal framework section.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of school computer equipment, schools should determine the level of response necessary for the offence disclosed. The decision to involve Police should be made as soon as possible if the offence is deemed to be out of the remit of the school to deal with. If schools are unsure if an issue is of a criminal nature then the Designated Safeguarding Lead should seek advice. Where it is determined that an offence has been committed and that a police investigation is warranted, all measures to preserve evidence should be undertaken. If an officer decides that equipment needs to be seized, then they will need to determine if the equipment is networked. If in doubt as to whether the server should be seized or not, officers should seek advice from the Police Digital Forensic Unit, as seizure of the server will have a significant impact on the school. It is essential that schools are aware of this possibility and they should ensure that measures are in place to enable the school's computer network to continue functioning should this situation arise. In cases where a suspect picture or photograph is discovered it should also be borne in mind that a person could be guilty of the offence to 'Make' and 'Distribute' if they print or forward the image.



Responding to concerns regarding radicalisation and extremism online

Schools and settings should be mindful of the specific responsibilities and requirements placed upon them under the Prevent Duty <https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty> From 1st July 2015 specified authorities, including all schools are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015 (“the CTSA 2015”), in the exercise of their functions, to have “due regard to the need to prevent people from being drawn into terrorism” This duty is known as the Prevent duty. The statutory Prevent guidance summarises the requirements on schools as undertaking risk assessment, working in partnership, staff training and IT policies.

Schools are expected to assess the risk of children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology which includes a range of extremism views including the far right. Schools should have clear procedures in place for protecting children who are identified to be at risk of radicalisation. These procedures may be set out in existing safeguarding policies and it is not necessary for schools and colleges to have distinct policies on implementing the Prevent duty. The online safety policy will be an important part of this role as it will highlight the action that the school will take to ensure that children are safe from terrorist and extremist material when accessing the internet in schools.

‘Keeping Children Safe in Education’ 2016 highlights that governing bodies should ensure that suitable filtering is in place which takes into account the needs of the schools community. Schools should ensure that online safety education highlights the risks of extremist content online, especially regarding the use and power of social media as a tool in radicalisation.

When ensuring appropriate filtering is in place, schools should be mindful to act in accordance with the law, much like when ensuring the filtering blocks other forms of illegal content. It should also be noted that radicalisation and extremist views can be shared and accessed on variety of platforms, including user generated or social media sites such as Facebook and YouTube and schools should make filtering decisions with this in mind. The way in which the monitoring of internet and network use is managed will be down to individual schools to decide and implement so as to meet their specific needs and requirements, for example taking into account the curriculum and also the needs and abilities of the community e.g. pupils or staff with EAL. The school (Head and Governing Body) needs to be able to satisfy itself that appropriate safeguarding measures (all reasonable precautions) are being taken to identify any activity which indicates that pupils or staff may be at risk of harm (or indeed putting others at risk). Leaders will need to ensure that appropriate time and resources are available to ensure that this is done sufficiently for a range of risks which will include radicalisation and extremism from a variety of perspectives as well as grooming and child sexual exploitation.

If schools/settings use devices which do not require pupils/staff to “login” to systems (such as iPads) to access the internet then they must ensure that there is appropriate mechanisms in place to log which member of the community has access to which devices to ensure that if concerns are identified, the school can trace users. Staff with the responsibility for managing and monitoring the school filtering and network must have appropriate resources available to them as well as training and support to ensure that this can be carried out in both a manageable and a safe way. These decisions must be documented within the appropriate school policies (especially the school AUP) and be supported with training etc. and supervision all staff involved as well as the wider whole school staff and pupil group.

Schools should always be aware that simply relying on filtering to prevent radicalisation will not be sufficient as children are likely to have access to a range of devices within the home which may not be filtered or monitored, education around safe use if therefore essential. As all safeguarding risks, all members of staff should be alert to changes in children’s behaviour which may indicate that they may be at risk or in need of specific help or protection. All members of staff should receive appropriate training to enable them to explore their responsibilities with regards to prevent for safeguarding pupils and adults within the school community.

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



Responding to concerns regarding cyberbullying

Online or cyberbullying can be defined as the use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone.

Cyberbullying is becoming increasingly prevalent with the rapid advances and use of modern technology. Mobile, internet and wireless technologies have increased the pace of communication and brought significant benefits to users worldwide but their popularity provides increasing opportunity for misuse through 'cyberbullying', with worrying consequences. It is crucial that children and young people as well as adults, use their devices and the internet safely and positively and they are aware of the consequences of misuse. As technology develops, bullying techniques can evolve to exploit it.

When children or adults are the target of bullying via mobile phones, gaming or the Internet, they can often feel very alone, particularly if those around them do not understand online bullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

Cyberbullying may not always be intentional and repeated in the same way that traditional offline bullying is. Repeated harassment online could include an initial concern which is then shared or endorsed by others such as by "liking", "sharing" or "commenting". People may not feel that they are bullying by doing this and single issue may become more serious. It is very important that all incidents of online abuse are addressed as early as possible to prevent escalation. Education staff, parents and young people have to be constantly vigilant and work together to prevent this and tackle it wherever it appears. Cyberbullying is a method of bullying and should be viewed and treated the same as "real world" bullying and can happen to any member of the school community.

'Keeping Children Safe in Education' 2016 highlights the need for staff to be aware that abuse can be perpetrated by children themselves including cyberbullying, and staff must be aware of concerning behaviour and appropriate safeguarding responses.

It is essential that young people, school staff and parents and carers understand how online can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety. There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:

- 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
- gives headteachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

Where online bullying which takes place outside school is reported then it must be investigated and acted on appropriately by schools.

Under the Children Act 1989 a bullying incident should be addressed as a child protection concern when there is 'reasonable cause to suspect that a child is suffering, or is likely to suffer, significant harm' and Emotional abuse highlights the impact of online bullying. Where this is the case, the school staff should report their concerns to the Education Safeguards Team. Even where safeguarding is not considered to be an issue, schools may need to draw on a range of external services to support the pupil who is experiencing bullying, or to tackle any underlying issue which has contributed to a child doing the bullying.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications both on and offline could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed they should seek assistance from the police. Additional advice and information can be found at <http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety/cyberbullying>

For more information please read "Preventing and Tackling Bullying: Advice for School Leaders, Staff and Governing Bodies" <https://www.gov.uk/government/publications/preventing-and-tackling-bullying>



Childnet International have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: www.childnet.com

Responding to concerns regarding online hate

Hate crimes are any crimes that are targeted at a person because of hostility or prejudice towards that person's disability

- race or ethnicity
- religion or belief
- sexual orientation
- transgender identity

Schools must ensure that they respond appropriately regarding online hate and discrimination and support members of the community who may be targeted online.

- **Useful links** 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

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

The following statements may help 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.
If the adult works with children or young people the LADO should also be informed
- 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?
- 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.**

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. 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)

Page | 17

Role/Author:

Policy Revision Date: 16th July, 2018

Approval Date:

Status:

Next Review Date: 16th July, 2019



(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 sadomasochism.

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.

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

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

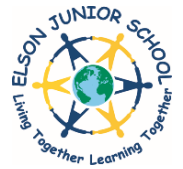
The Marie Collins Foundation: <http://www.mariecollinsfoundation.org.uk/>

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

Elson Junior School

eSafety Policy



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/>



APPENDIX TWO

e-Safety Incident Log

Number:	Reported By: <i>(name of staff member)</i>	Reported To: <i>(e.g. Head, e-Safety Officer)</i>	
	When:	When:	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		Date:	
Signature (Governor)		Date:	



APPENDIX THREE

Risk Log

(with a couple of examples)

No.	Activity	Risk	Likelihood	Impact	Score	Owner
1.	Internet browsing	Access to inappropriate/illegal content - staff	1	3	3	e-Safety Officer IT Support
1.	Internet browsing	Access to inappropriate/illegal content - students	2	3	6	
2.	Blogging	Inappropriate comments	2	1	2	
2.	Blogging	Using copyright material	2	2	4	
3.	Student laptops	Students taking laptops home – access to inappropriate/illegal content at home	3	3	9	

Likelihood: How likely is it that the risk could happen (foreseeability).

Impact: What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)

Likelihood and Impact are between 1 and 3, 1 being the lowest.

Multiply Likelihood and Impact to achieve score.

LEGEND/SCORE: 1 – 3 = **Low Risk**
 4 – 6 = **Medium Risk**
 7 – 9 = **High Risk**

Owner: The person who will action the risk assessment and recommend the mitigation to Headteacher and Governing Body.
 Final decision rests with Headteacher and Governing Body

APPENDIX FOUR: Risk Assessment

Risk No.	Risk
3	In certain circumstances, students will be able to borrow school-owned laptops to study at home. Parents may not have internet filtering applied through ISP. Even if they do there is no way of checking the effectiveness of this filtering; students will potentially have unrestricted access to inappropriate/illegal websites/services. As the laptops are owned by the school, and the school requires the student to undertake this work at home, the school has a common law duty of care to ensure, as much as is reasonably possible, the safe and well being of the child.
Likelihood	The inquisitive nature of children and young people is that they may actively seek out unsavoury online content, or come across such content accidentally. Therefore the likelihood is assessed as 3.
3	
Impact	The impact to the school reputation would be high. Furthermore the school may be held vicariously liable if a student accesses illegal material using school-owned equipment. From a safeguarding perspective, there is a potentially damaging aspect to the student.
3	
Risk Assessment	HIGH (9)
Risk Owner/s	e-Safety Officer IT Support
Mitigation	<p>This risk should be actioned from both a technical and educational aspect:</p> <p>Technical: Laptop is to be locked down using XXXXXXXX software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet. The outcome is that the student will receive the same level of Internet filtering at home as he/she gets whilst in school.</p> <p>Education: The e-Safety Policy and Acceptable Use Policy will be updated to reflect the technical mitigation. Both the student and the parent will be spoken to directly about the appropriate use of the Internet. Parents will be made aware that the laptop is for the use of his/her child only, and for school work only. The current school e-safety education programme has already covered the safe and appropriate use of technology, students are up to date and aware of the risks.</p>

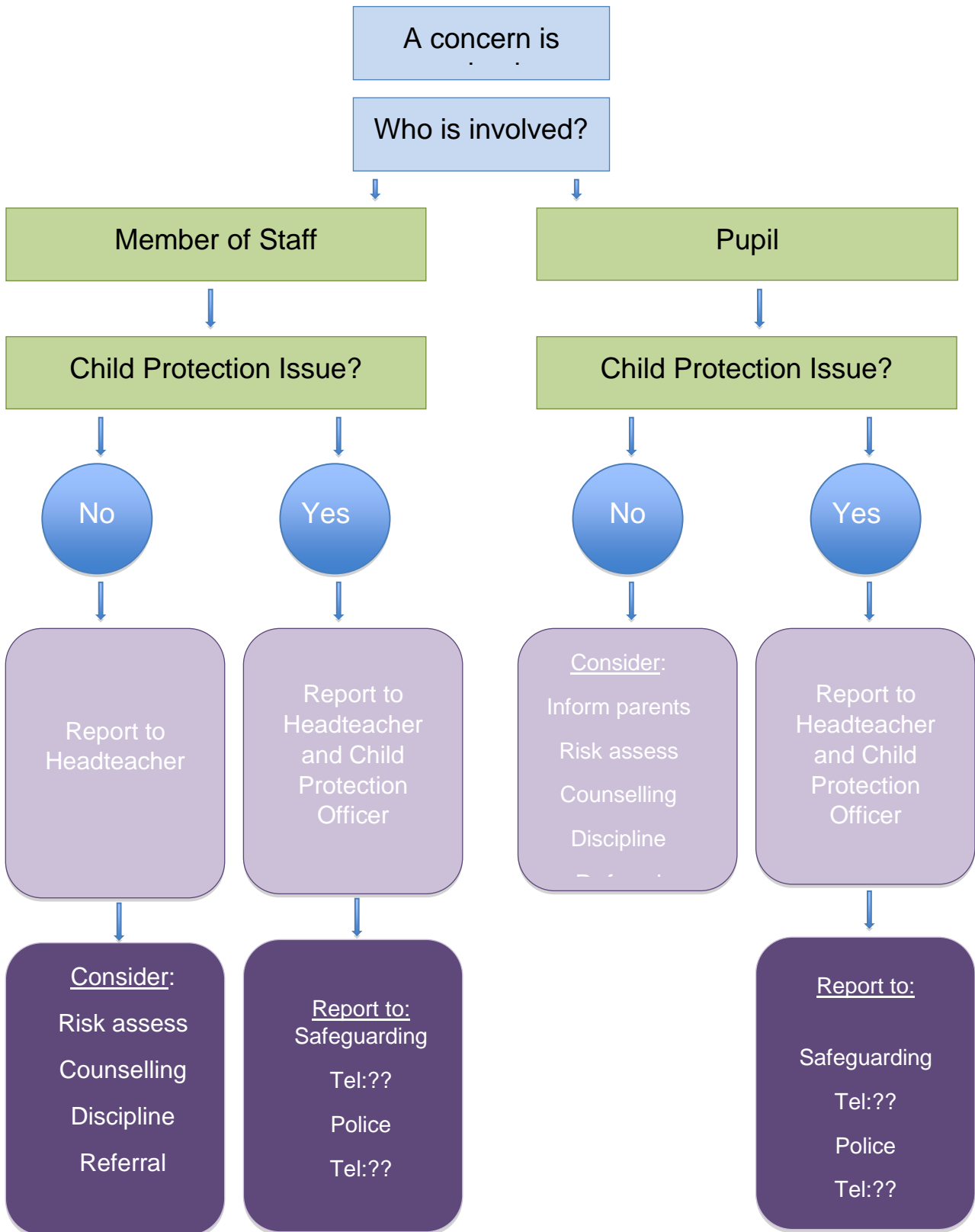
Approved /Not Approved (circle as appropriate)

Date:

Signed (Headteacher):

Signed (Governor):

APPENDIX FIVE: Inappropriate Activity Flowchart



If you are in any doubt, _ the Headteacher, Child Protection Officer or Safeguarding

APPENDIX SIX

Illegal Activity Flowchart

