



Neston Primary School

Online Safety Policy

2022-2023



Contents

Neston Primary School Online Safety Policy	1
Development Review of this Policy	4
Schedule for Development	4
1. Aims	5
Scope of the Policy	5
Roles and Responsibilities	6
Governors	6
Headteacher and Senior Leaders	6
The ICT Manager and Computing Lead	7
All Staff and Volunteers	7
Designated Safeguarding Lead - Helen Pillinger	7
Pupils:	8
Parents / Carers	8
Cyber Bullying	9
Policy Statements	10
Education – Pupils	10
Education – Parents / Carers	11
Training	11
Technical – infrastructure / equipment, filtering and monitoring	12
Use of digital and video images	13
Data Protection	14
Communications	15
Dealing with unsuitable / inappropriate activities	15
Illegal Incidents	17
Other Incidents	18
School Actions & Sanctions	19
Appendix	21



Acknowledgements 22

Responsible Internet Use 23

RE: Responsible Internet Use Agreement..... 24

RE: Consent for Processing Personal Data..... 25

Legislation 28

Links to other organisations or documents..... 33

Glossary of Terms..... 36



Development Review of this Policy

This Online Safety policy has been developed by a working group made up of:

- Headteacher
- Online Safety Lead
- Online Safety Governor
- Staff – including Teachers, Support Staff
- Governors
- Parents and Carers

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development

This Online Safety policy was approved by the Governing Body on:	Oct 2022
The implementation of this Online Safety policy will be monitored by the:	Headteacher Pam Evans, Online Safety Lead Natasha Patrick, Online Safety Governor John Andrews, Senior Leadership Team, and the Governing Body
Monitoring will take place at regular intervals:	Annually
The Governing Body / Governors Sub Committee will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Governor’s - Curriculum, Standards & School Improvement (CSSI) Committee will receive updates at each committee meeting and review annually
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Oct 2023
Should serious online safety incidents take place, the following external persons / agencies should be informed:	DSL, DDSL, LA, Safeguarding Officer, MASH, LADO, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
 - students / pupils



- parents / carers
- staff

1. Aims

- Our school aims to:
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- **The 4 key categories of risk**
- Our approach to online safety is based on addressing the following categories of risk:
- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behavior that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Scope of the Policy

This policy applies to all members of the Neston Primary School community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.



Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is John Andrews.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority / other relevant body disciplinary procedures).
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.



The ICT Manager and Computing Lead

- The ICT manager is responsible for:
- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- This list is not intended to be exhaustive.

All Staff and Volunteers

- All staff, including contractors and agency staff, and volunteers are responsible for:
- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- This list is not intended to be exhaustive.

Designated Safeguarding Lead - Helen Pillinger

Deputies – Pam Evans and Natasha Patrick

- Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.
- The DSL takes lead responsibility for online safety in school, in particular:
- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents



- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- This list is not intended to be exhaustive.

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature*. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / Learning Platform and on-line pupil records



Cyber Bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules
- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
 - Delete that material, or
 - Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
 - Report it to the police*
- Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.
- Any searching of pupils will be carried out in line with:
- The DfE's latest guidance on [screening, searching and confiscation](#)



- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- The school's COVID-19 risk assessment
- Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE and RSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.



In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Pupils in **Key Stage 2** will be taught to:
 - Use technology safely, respectfully and responsibly
 - Recognise acceptable and unacceptable behaviour
 - Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, web site, Learning Platform*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications e.g. [swgfl.org.uk](http://www.swgfl.org.uk)
www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>*

Training

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).



- By way of this training, all staff will be made aware that:
- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
- Training will also help staff:
 - develop better awareness to assist in spotting the signs and symptoms of online abuse
 - develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
 - develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term
 - The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
 - Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
 - Volunteers will receive appropriate training and updates, if applicable.
 - More information about safeguarding training is set out in our child protection and safeguarding policy.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- The "master / administrator" passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)



- School Care is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- **Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.**
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press.
- In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the GDPR). To respect everyone’s privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.



- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school / academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO). The school may also wish to appoint a Data Manager and systems controllers to support the DPO.
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice. (see Privacy Notice section in the appendix)
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.



- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The school currently considers the risk / disadvantages do not outweigh the benefit of using these technologies for education

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:



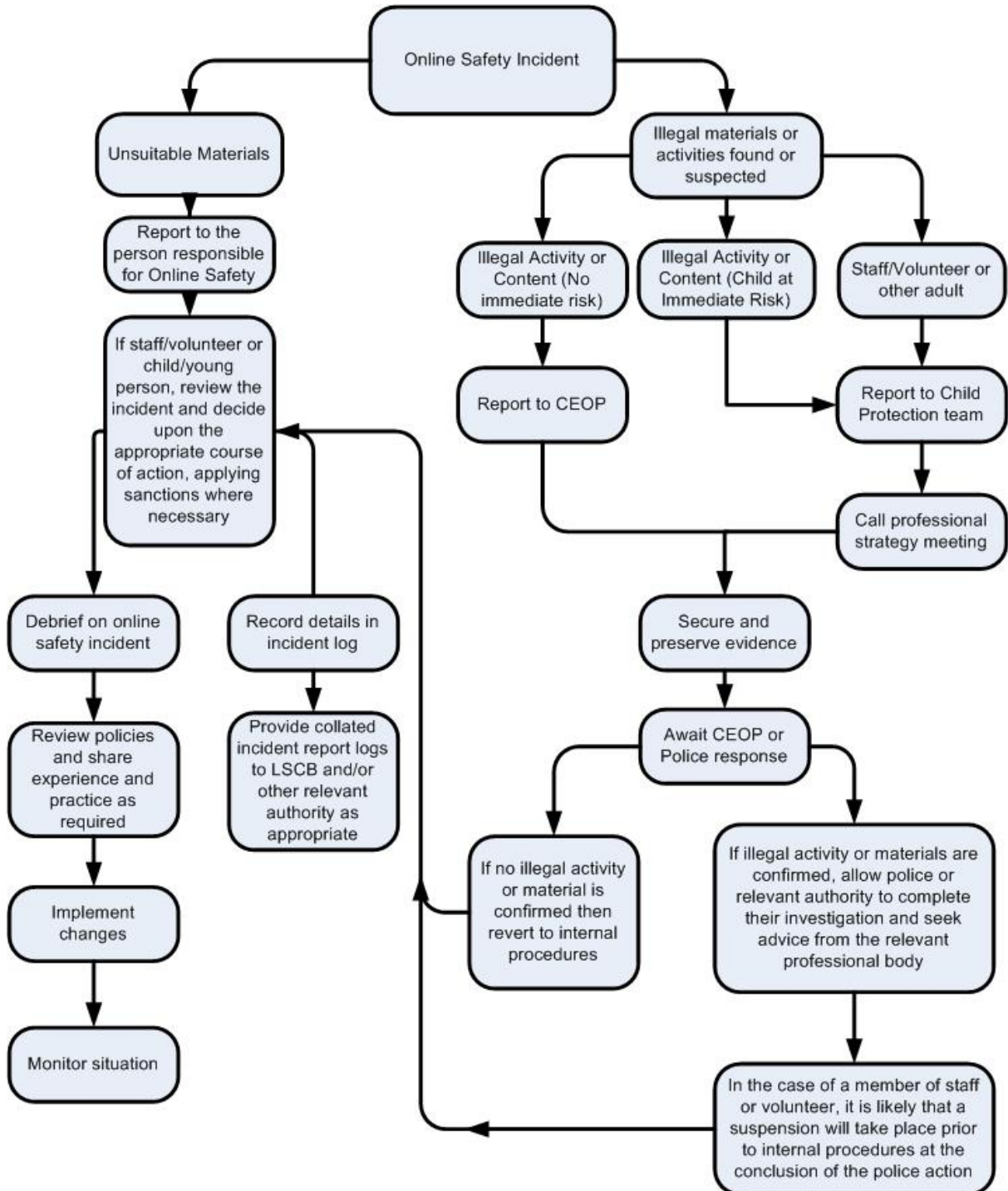
User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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 kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X		
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X		
Infringing copyright				X		
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X		
Creating or propagating computer viruses or other harmful files				X		
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X		



Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.





Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority Group or national / local organisation (as relevant).
 - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - promotion of terrorism or extremism
 - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the *school / academy* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.



School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Actions / Sanctions

Pupils Incidents	Actions / Sanctions								
	Refer to class teacher / tutor	Refer to Head of Department / Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X		X			X		X	X
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X		X			X		X	X
Unauthorised downloading or uploading of files	X		X		X	X		X	X
Attempting to access or accessing the school network, using the account of a member of staff	X		X			X		X	X
Corrupting or destroying the data of other users	X		X			X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X		X	X	X	X			



Actions / Sanctions

Staff Incidents

	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Deliberate actions to breach data protection or network security rules	X	X	X			X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X			X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X			X	X	X
Actions which could compromise the staff member's professional standing	X	X	X			X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school / academy	X	X	X			X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X	X			X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X					
Deliberately accessing or trying to access offensive or pornographic material	X	X	X			X	X	X
Breaching copyright or licensing regulations	X	X	X					
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X	X	X



Appendix

Copies of the Neston Primary School Responsible Internet Use poster and other template and agreements, contained in the appendices

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	



Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template and of the 360 degree safe Online Safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Copyright of these Template Policies is held by SWGfL. Schools / Academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy writing, review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in April 2018. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

© South West Grid for Learning Trust Ltd 2018



Responsible Internet Use

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will use only my class network login and password.
- I will only open or delete my own files.
- I understand that I must not bring into school and use software or files without permission.
- I will only e-mail and open attachments from people I know, or my teacher has approved during guided sessions.
- The messages I send will be polite and sensible and only during guided sessions.
- I understand that I must **never** give my home address or phone number or arrange to meet someone.
- If I see anything, I am unhappy with or I receive messages I do not like, I will tell a teacher **immediately**.
- I understand that the school may check my computer files, e-mails I send and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

School Care monitors all Internet use and will notify the police and Local Authority if an illegal website is accessed.



To: All Parents/Guardians of Neston School Pupils

RE: Responsible Internet Use Agreement

As part of your child’s curriculum and the development of Information Technologies skills, Neston Primary School provides supervised access to the internet. We believe that the effective use of the Internet and e-mail is worthwhile and is an essential skill for children as they grow up in our modern world. We ask that you please review the rules for Responsible Internet Use. Please read and share with your child the rules below and sign and return the form as soon as possible.

As a school we use an education broadband provider ‘School Care’ that operates a filtering system which restricts access to inappropriate materials therefore reducing risk to pupils. Whilst every endeavour has been made to ensure children are not at risk, we also appreciate that the Internet is constantly evolving and therefore there is always a possibility of risk involved. To mitigate this risk, one of the aims of our IT curriculum is to ensure your child knows how to deal appropriately with any issues that may arise.

Should you wish to discuss any aspect of internet use, please do not hesitate to speak to your class teacher.

Pam Evans

Head Teacher



<p>Pupil</p> <p>I will use the computer systems and internet in school responsibly and follow the school rules at all times.</p>	<p>SIGN HERE</p>
<p>Parent</p> <p>I give permission for my child to access the internet under supervised conditions at school. I understand that the school cannot be held responsible for the nature or content of materials accessed through the internet which are out of our filtering controls</p>	<p>SIGN HERE</p>

Parent/Carer’s Name: Signature

On behalf of.....(child’s name)

Date:

For more information about how your child’s personal data is used, including their rights as a data subject, please see our privacy notice at <http://nestonprimary.co.uk/data-protection>



To: All Parents/Guardians of Neston School Pupils

RE: Consent for Processing Personal Data

We use consent as our basis to process your child’s personal data in certain circumstances. This form details the activities in which we use consent. Please note there are certain activities where we do not use consent as the basis for processing your child’s data. These are described in our Privacy Notices which can be found on our website <http://nestonprimary.co.uk/data-protection> and which are available in hard copy form from the School Office.

Please also note:

- Unless you have given your express consent, we will never put a child’s full name alongside any published image.
- Videos may be taken of lessons to support staff development; these may be seen by other teachers in school for staff training.
- We may also take photos/video of your child for identification purposes, and for evidencing their educational development. Such data will sit on their file and not be shared unless the law requires us to do so, or you have given your specific consent.
- Parents / carers are welcome to take videos and photos of **their** children at school events for **their own personal use**. However, to respect everyone’s privacy rights and in some cases protection, these images **should not** be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the images / footage.
- Websites and social media can be viewed throughout the world and not just in the United Kingdom, where UK law applies. When images are posted on the internet, it is not possible to prevent others from reposting them.
- Additional and specific consent for use by external agencies/companies may be sought.

Please be aware you can withdraw consent at any time. If you have any queries or wish to withdraw, or review your consent you can contact the school office.

Pupil Name	Class			
I give my permission:			I consent (Yes / ✓)	I do not consent (No / ✗)
For images or video footage of my child to be used in the school on activity boards, screens, reception area for promotional purpose. <i>Note: this is separate to our statutory obligation to display your child’s work around the school, which may contain their personal information. We do not require your consent to do this.</i>				
For images or video footage of my child to be used on the school website for publicity purposes: http://nestonprimary.co.uk/				
For images or footage of my child to be used on social media : Facebook, Twitter, Instagram <i>Note: our social media accounts are open pages.</i>				
For images or video footage of my child to be used in printed materials such as the school newsletter or the school prospectus.				
For images or video footage of my child to be used in the media (local / national press) . We will only print their name in exceptional circumstances, and with your permission.				
For the school to contact me to obtain feedback on the school and how we can improve.				
For the school to contact me with regards activities, events and offers , for example PTA, friends of school, local groups, book offers. <i>Note: we will contact you to keep you up to date with school notices and information. We do not require your consent to do this.</i>				
We also use a third party as a school photographer. They come into school, take pictures of your child (and their siblings), and pass them back to us. We then distribute these proofs to you, so you can decide whether to purchase the photo directly from the photographer. If you would like further information about the photographers GDPR, please contact the school.				

It is assumed that you (and each of you with parental responsibility for your child) have consulted with each other so far as the completion of this form and the giving of consents is concerned.

Name of person completing this form		Relationship to child	
Signed:		Dated:	



Neston Primary School Laptop policy

1. The laptop remains the property of Neston Primary School.
2. The laptop is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only Neston Primary School Staff should use the laptop.
3. On the teacher leaving the school's employment, the laptop is returned to Neston Primary School. Staff on extended leave of 4 weeks and over should return their laptops to the school (other than by prior agreement with the Head Teacher).
4. When in school and not being used, the laptop must be kept in an office, locked room or drawer. It must not be left in an unlocked, unattended classroom.
5. Whenever possible, the laptop must not be left in an unattended car. If there is a need to do so it should be locked in the boot.
6. The laptop must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the Head Teacher with evidence of adequate insurance.
7. Staff may load their own software onto the laptop, but it must be fully licensed and not corrupt any software or systems already installed on the laptop.
8. Any software loaded must not affect the integrity of the school network.
9. If any removable media is used, then it must be checked to ensure it is free from any viruses.
10. It will be the responsibility of the member of staff to ensure virus protection software that has been installed on the laptop is kept up-to-date.
11. Staff must use their laptop in school on the network at least once a week to ensure virus protection is automatically updated.
12. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
13. Students must never use the laptop.
14. If any fault occurs with the laptop, it should be referred immediately to the Network Manager.
15. When being transported, the carrying case supplied must be used at all times.
16. The laptop would be covered by normal household insurance. If not, it should be kept in school and locked up overnight.

Policy for responsible e-mail, network and Internet use for Neston Primary School

1. I will use all Information Communication Technologies (ICT) equipment issued to me in an appropriate way. I will not:
 - Access offensive website or download offensive material.
 - Make excessive personal use of the Internet or e-mail.
 - Copy information from the Internet that is copyright or without the owner's permission.
 - Place inappropriate material onto the Internet.
 - Will not send e-mails that are offensive or otherwise inappropriate.
 - Disregarded my responsibilities for security and confidentiality.
 - Download files that will adversely affect the security of the laptop and school network.
 - Access the files of others or attempt to alter the computer settings.
 - Update web pages etc. or use pictures or text that can identify the school, without the permission of the Head Teacher.
 - Attempt to repair or interfere with the components, software or peripherals of any computer that is the property of Neston Primary School.



2. I will only access the system with my own name and registered password, which I will keep secret.
3. I will inform the Network Manager/School's Technician as soon as possible if I know my password is no longer secret.
4. I will always log off the system when I have finished working.
5. I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the Internet sites I visit.
6. My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the Head Teacher and register the passwords with the Head Teacher.
7. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.
8. I will always adhere to Neston Primary School Software Compliance Policy.
9. I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the Network Manager.
10. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.
11. I will report immediately to the Head Teacher any unpleasant material or messages sent to me.
12. I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.
13. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
14. Storage of e-mails and attachment should be kept to a minimum to avoid unnecessary drain on memory and capacity.
15. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
16. I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow.

Name

Signature:

Date:

I have read and understood our school Online Safety Policy



Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

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, they have to follow a number of set procedures.

Communications Act 2003

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.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
 - Ascertain whether the communication is business or personal;
 - Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

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, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. 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. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g., YouTube).

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.



Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

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.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he 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.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

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. Children, Families and Education Directorate page 38 April 2007.



Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights 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. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and 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. ([see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation](http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation))

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)



Equality Act 2010: guidance

Information and guidance on the Equality Act 2010, including age discrimination and public sector Equality Duty.

[Equality Act 2010: guidance - GOV.UK \(www.gov.uk\)](http://www.gov.uk)

Statutory Guidance

Department for Education – Keeping Children Safe in Education 1 September 2022. Statutory guidance for schools and colleges on safeguarding children and safer recruitment.

[DfE – Keeping Children Safe in Education](#)



Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy:

UK Safer Internet Centre

Safer Internet Centre – <https://www.saferinternet.org.uk/>

UK Council for Internet Safety (UKCIS) guidance: [Education for a connected world](#)

UKCIS guidance: [Sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

The UKCIS [external visitors guidance](#) will help schools and colleges to ensure the maximum impact of any online safety sessions delivered by external visitors

South West Grid for Learning - <https://swgfl.org.uk/products-services/online-safety/>

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Internet Watch Foundation - <https://www.iwf.org.uk/>

DfE advice for schools: [teaching online safety in schools](#)

Public Health England: [Every Mind Matters](#)

[Harmful online challenges and online hoaxes](#) - this includes advice on preparing for any online challenges and hoaxes, sharing information with parents and carers and where to get help and support.

CEOP

National Crime Agency's CEOP education programme

CEOP - <http://ceop.police.uk/>

[ThinkUKnow](https://www.thinkuknow.co.uk/) - <https://www.thinkuknow.co.uk/>

The Children's Society in partnership with Victim Support and National Police Chiefs' Council - [County Lines – Children's Society toolkit for professionals \(yjlc.uk\)](#)

Others

[LGfL – Online Safety Resources – \(LGfL 'Undressed' provided schools advice about how to teach young children about being tricked into getting undressed online in a fun way without scaring them or explaining the motives of sex offenders\)](#)

[Kent – Online Safety Resources page](#)

INSAFE / Better Internet for Kids - <https://www.betterinternetforkids.eu/>

UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis

Netsmartz - <http://www.netsmartz.org/>

Tools for Schools

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

360Data – online data protection self-review tool: www.360data.org.uk



Bullying / Online-bullying / Sexting / Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour - <http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance -

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>

[Childnet – Project deSHAME – Online Sexual Harrassment](#)

[UKSIC – Sexting Resources](#)

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

[Ditch the Label – Online Bullying Charity](#)

[Diana Award – Anti-Bullying Campaign](#)

Social Networking

Digizen – [Social Networking](#)

UKSIC - [Safety Features on Social Networks](#)

[Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media](#)

Curriculum

[SWGfL Digital Literacy & Citizenship curriculum](#)

[UKCCIS – Education for a connected world framework](#)

Teach Today – www.teachtoday.eu/

Insafe - [Education Resources](#)

Mobile Devices / BYOD

Cloudlearn Report [Effective practice for schools moving to end locking and blocking](#)

NEN - [Guidance Note - BYOD](#)

Data Protection

[360data - free questionnaire and data protection self-review tool](#)

[ICO Guide for Organisations \(general information about Data Protection\)](#)

[ICO Guides for Education \(wide range of sector specific guides\)](#)

[DfE advice on Cloud software services and the Data Protection Act](#)

[ICO Guidance on Bring Your Own Device](#)

[ICO Guidance on Cloud Computing](#)

[ICO - Guidance we gave to schools - September 2012](#)

[IRMS - Records Management Toolkit for Schools](#)

[NHS - Caldicott Principles \(information that must be released\)](#)



[ICO Guidance on taking photos in schools](#)

[Dotkumo - Best practice guide to using photos](#)

Professional Standards / Staff Training

[DfE – Keeping Children Safe in Education {1 September 2022}](#)

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)

[Childnet – School Pack for Online Safety Awareness](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

Infrastructure / Technical Support

[UKSIC – Appropriate Filtering and Monitoring](#)

Somerset - [Questions for Technical Support](#)

NEN – [Advice and Guidance Notes](#)

Working with parents and carers

[SWGfL Digital Literacy & Citizenship curriculum](#)

[Online Safety BOOST Presentations - parent's presentation](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops / education](#)

[The Digital Universe of Your Children - animated videos for parents \(Insafe\)](#)

[Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide](#)

[Insafe - A guide for parents - education and the new media](#)

Research

[EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011](#)

[Futurelab - "Digital participation - its not chalk and talk any more!"](#)

[Ofcom –Media Literacy Research](#)



Glossary of Terms

AUP / AUA	Acceptable Use Policy / Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,



WAP Wireless Application Protocol

UKSIC UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in April 2016. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal / professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.