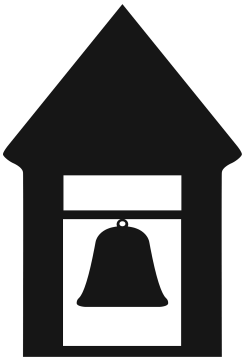


Hague Bar Primary School
& *PEGS*

Policy for

Online-Safety and Acceptable Use Policy

REVIEWED: November 2017

Hague Bar Primary School
Shared policy with PEGS

Online-Safety and Acceptable Use Policy

Aims of policy

- Hague Bar Primary School believes that online safety is an essential element of safeguarding children and adults in the digital world when using technology such as computers, tablets, mobile phones or games consoles. Internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.
- We have a duty to provide the school community with quality Internet access to raise education standards, enrich learning, support professional work of staff and enhance management functions.
- We are responsible for ensuring that the school IT infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.
- The school identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.
- The purpose of this online safety policy is to:
    - Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that the school is a safe and secure environment for all;
    - Safeguard and protect all members of the school community online;
    - Raise awareness with all members of the school community regarding the potential risks as well as benefits of technology;
    - Enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology;
    - Identify clear procedures, known by all members of the community, to follow when responding to online safety concerns or breach of policy.
- This policy applies to all staff including the governing board, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school, as well as children and parents/carers.
- This policy applies to all access to the Internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as laptops, tablets or mobile phones.

- This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour and discipline, data security, use of images, confidentiality, staff code of conduct, and relevant curriculum policies including Computing, Personal Social and Health Education (PSHE) and Relationships and Sex Education (RSE).

Contents of this policy

This document will be split up into the following sections:

This online-safety policy was approved in principle by the full Governing Board on:	Autumn 16 Safeguarding Committee meeting.
The implementation of this online-safety policy will be monitored by the:	**Online-Safety Lead: Sue kennedy** **Safeguarding DSL: Sue Kennedy** **Deputy DSL: John Groarke/Any PEGS DSL** **Safeguarding Governor: Caroline Liles**
Monitoring will take place at termly intervals:	**Beginning of each term**
The Safeguarding Governing Board will receive a report on the implementation of the online-safety policy generated by the monitoring group (which will include anonymous details of any online-safety incidents) at regular intervals:	**Annually in Autumn, through the Headteacher's Report to Governors.**
The Online-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technologies, new threats to online-safety or incidents that have taken place. The next anticipated review date will be:	**Annually – see Safeguarding Governor meeting schedule**
Should serious online-safety incidents take place, the following persons should be informed:	**Safeguarding DSL: Sue Kennedy (Head)**
Monitoring/development team for online-safety:	**Headteacher/DSL: Sue Kennedy** **Deputy DSL: Rachel Parry**

	Computing Lead: Kai Julier **Governor for safeguarding: COG Dan Riley** **IT Consultant/Technician: Ian Burke**

Key responsibilities of users

The key responsibilities of the school management and leadership team are to:

- Develop, own and promote the online safety vision and culture to all stakeholders, in line with national and local recommendations.
- Ensure that online safety is viewed by the whole community as a safeguarding issue, and proactively develop a robust online safety culture.
- Support the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensure there are appropriate and up-to-date policies and procedures regarding online safety in place, including an Acceptable Use Policy.
- Ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content and which meet the needs of the school community, whilst ensuring children have access to required educational material.
- Work with and support technical staff in monitoring the safety and security of school systems and networks and to ensure that the school network system is actively monitored.
- Ensure all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- Be aware of any online safety incidents and ensure that external agencies and support are liaised with, as appropriate.
- Receive and regularly review online safeguarding records and use them to inform and shape future practice.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including the safe and responsible use of devices.
- To ensure a member of the Governing Board is identified with a lead responsibility for supporting online safety (the safeguarding governor at Hague Bar).
- Audit and evaluate current online safety practice to identify strengths and areas for improvement.

The key responsibilities of the Designated Safeguarding Lead are to:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff and other agencies, as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety.
- Coordinate participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.

- Ensure that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches, e.g. the school website, Newsletters, Facebook, Twitter.
- Ensure that practice is in line with current legislation regarding data protection and data security.
- Maintain a record of online safety concerns/incidents and actions taken as part of the school's safeguarding recording procedures. (My Concern)
- Monitor the school's online safety incidents to identify gaps/trends and use this data to update the school's response to reflect need.
- Report online safety concerns data to the Governing Board and other agencies, as appropriate.
- Liaise with the local authority and other local and national bodies, as appropriate.
- Ensure that this policy and other related policies are reviewed, with stakeholder input, on a regular basis (at least annually).

The key responsibilities of all members of staff are to:

- Contribute to the development of the online safety policy and other related policies.
- Read the school Acceptable Use Policies (AUPs) and adhere to them.
- Take responsibility for the security of school systems and data.
- Have an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Model good practice when using new and emerging technologies.
- Embed online safety education in curriculum delivery – in line with the Personal Safety curriculum and as situations arise.
- Identify individuals of concern and take appropriate action by following school safeguarding policies and procedures.
- Know when and how to escalate online safety issues, internally and externally.
- Signpost to appropriate support available for online safety issues, internally and externally.
- Maintain a professional level of conduct in their personal use of technology, both on and off site.
- Demonstrate an emphasis on positive online learning opportunities.
- Take personal responsibility for professional development in this area.

The key responsibilities of the IT technician are to:

- Provide a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised.
- Take responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- Ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensure that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Ensure that the use of the school's network is regularly monitored and report any deliberate or accidental misuse to the DSL.
- Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.

- Develop an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaise with the local authority, as appropriate, on technical infrastructure issues.
- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensure that the school's ICT system is secure and not open to misuse or malicious attack.
- Ensure that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced, as appropriate.

The key responsibilities of pupils are to:

- Contribute to the development of the online safety policy.
- Read the school's Acceptable Use Policy and sign to acknowledge agreement to adhere to the statements therein.
- Respect the feelings and rights of others both on and offline.
- Seek help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- At a level that is appropriate to their individual age, ability and vulnerabilities:
  - Take responsibility for keeping themselves and others safe online.
  - Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
  - Assess the personal risks of using any particular technology, and behave safely and responsibly to limit those risks.

The key responsibilities of parents and carers are to:

- Read the school's Acceptable Use Policy, encouraging their children to adhere to them, and adhere to them themselves, where appropriate.
- 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, and liaise with the school about such concerns.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contribute to the ongoing development of this policy.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- In accordance with guidance from the Information Commissioner's Office, ensure that videos and digital images taken of their children at school events are for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images will not be published or made publicly available on social networking sites. At the

beginning of school events, parents should be reminded about the Use of Images Policy Agreement they have signed.

Technical Security

- Appropriate security measures are in place to protect school systems from accidental or malicious attempts which may threaten the security of the school systems and data.
- Servers and wireless systems are to be securely located and physical access restricted.
- The ICT Technician is responsible for ensuring that software license 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.
- All computers and devices in school should be locked down to keep them safe and should have access to the school's filtering systems.
- Any potential threats to safety or security should be reported to a member of the Senior Management Team immediately.
- Records of all users and rights to be audited and kept by the ICT Technician.
- 'Guest' users should be provided with separate login details (e.g. student teachers, supply teachers).
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious attacks and viruses.
- Any filtering issues should be reported immediately to the filtering provider, and the Online-Safety Lead and ICT Technician should be notified.
- Changes to the filtering system should be checked and audited.
- Any websites that have been accessed that included inappropriate content should be logged, reported and investigated.

Password security

- All adults and KS2 children will be given their own username and password.
- Passwords for new users, and replacement passwords for existing users will be allocated by the ICT Technician.
- All users have clearly defined access rights to school systems.
- The administrator passwords for the school will be made available for technical staff and the Headteacher/Online Safety Lead.
- All staff to have their passwords changed in the event of a breach of privacy.
- Passwords should be different for different systems and must be secure.

Acceptable Use Policy Agreement

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, iPads, mobile phones, tablets, digital cameras, email and social media sites**.**
I understand that any hardware or software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
I understand that the school will monitor my use of ICT systems, email and other digital communications.
I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may see it or have access to it.
I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the systems manager.
I will immediately report any illegal, inappropriate or harmful material or incident that I become aware of to the online-safety designated lead.
I will engage in social media (including social networking sites, blogs, wikis, forums, online gaming, video/photo sharing sits, chatrooms, instant messenger etc) always in a positive, safe and responsible manner at all times.
I will carefully consider the information, including text and images, I share and post online to ensure that my social media use is compatible with my professional role and is in accordance with school policies (safeguarding, anti-bullying, code of conduct, confidentiality, data protection etc).
I will not discuss work related matters on social media that could bring the school into disrepute.

I will not publish any content on social media that may be considered threatening, hurtful or defamatory to thoughts.
I will not share or discuss any information or content available to me as part of my employment, including photos and personal information about children and their families, on my personal social media sites.
I will not visit social media sites during school working hours for personal use.
I understand that personal opinions should not be attributed to the school community and should not bring the school, or anyone connected to it, into disrepute.
I will regularly check security settings on personal social media profiles to minimise the loss of personal information.
I will use my work email address to communicate with others about work-related matters. I will not give out my personal email address to anyone for the purpose of communicating about work related matters unless I have no other method of communication and wish to use my personal address for communication with SLT.

I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
I will communicate with others in a professional manner; I will not use aggressive or inappropriate language. I will appreciate that others may have different opinions.
I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's use of images policy. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured. Photographs taken in school are the property of the school and should not be downloaded onto my own equipment without express permission from the Headteacher and they should not be stored on my equipment.
I will never use chat and social networking on my own devices during working hours.
I will only communicate with pupils using official school systems and no forms of social media. Any such communication will be professional in tone and manner.
I will not engage in any online activity that may compromise my professional responsibilities or the good name of the school.

I will ensure that all devices brought from home will be free from any inappropriate content and only used with the permission of the Headteacher/Online-Safety Lead.
I will ensure that any devices used in school are given to the network technician to ensure they use the school filtering system.
Any device loss, theft or change of ownership will be reported to the Online-Safety Lead.
I will ensure that I have taken all the appropriate measures to keep my devices virus-free (install virus-software, choose a secure operating system etc.)
I will ensure that I have permission to use the original work of others in my own work.
Where work is protected by copyright, I will not download or distribute copies (including music, videos, software).

When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will always seek permission of the headteacher before using my own mobile devices. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses. Chargers should be PAT tested.
In lessons where Internet use is pre-planned pupils will be guided to sites checked as suitable for their use, and processes will be in place for dealing with any unsuitable material that is found in Internet search, i.e. turn the monitor off, close the laptop immediately and report to the teacher.
I will use my school email address on the school ICT systems. In some cases my personal email may be used, but only by agreement with the Headteacher.
l will take care when opening hyperlinks in emails, or attachments to emails, ensuring that the source is known and trusted. If I have any concerns about the validity of the email (due to the risk of viruses or other harmful programs attached), I will not open the attachments or hyperlinks.
I will not upload, download or access any material that is illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or any inappropriate material that may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials – if this happens or I inadvertently access inappropriate material then I will immediately report it to the Headteacher/Online-Safety Lead.
I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings. I will not disable or cause any damage to school equipment, or the equipment belonging to others.
I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school's Data Protection Policy. Where digital personal data is transferred outside the secure

local network, it must be encrypted. Paper-based Protected and Restricted data is held in lockable storage.
I understand that the data protection policy requires that any staff or pupil data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by the school policy to disclose such information to an appropriate authority (freedom of information policy).
I will immediately report to the Headteacher/Online-Safety Lead any damage or faults I know about involving ICT equipment or software, however this may have happened.

When using digital images, I will inform and educate pupils about the risks associated with taking, using, sharing, publishing and distributing images. I recognise the risks attached to publishing my own images on the internet e.g. on social networking sites.
I understand that I am allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Images should only be taken on school equipment; the personal equipment of staff, e.g. mobile phone camera, should not be used for such purposes, unless express permission is given by the headteacher – in which case all images should be transferred to school equipment and removed from personal equipment asap.
I shall take care when taking digital / video images to ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
I will ensure that photographs I publish on the website, or elsewhere that include pupils, will be selected carefully and will comply with expectations of good practice in school.
I will ensure that I do not post photographs on the school website of any pupils who do not have parental consent for photographs of them to be published.
I will ensure that pupils' full names are not be used anywhere on a website or blog, particularly in association with photographs.

Staff Online-Safety Acceptable Use Agreement

I understand that I am responsible for my actions in and out of the school.

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include being given a warning. The matter may be referred to the Governors at the school for a decision on disciplinary action which may involve suspension or dismissal. The Local Authority may be involved, and in the event of illegal activities there will be the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed / Date

The Internet Service Provider used by this school provides a continually updated, filtered service to attempt to ensure that only Internet sites suitable for children are available.

This is how we stay safe when we use computers:

- I will ask a teacher or adult if I want to use the computers.
- I will only use activities that the teacher or adult has told me to use.
- I will always take care of the computers and other equipment.
- I will ask for help from the teacher or adult if I am not sure what to do or if I think I have done something wrong.
- I will tell the teacher or adult if I see something that upsets me, or I think is wrong, on the screen. I will turn off the screen or lower the lid on the laptop if this happens.
- I know that if I break the rules I might not be allowed to use a computer by myself.
- I will only bring in computer games or files from home (DVD, memory stick etc) with permission from my teacher.
- I will always be kind and respectful online.

Signed (child): .....

As the parent / carer of the above pupil, I give permission for my son / daughter to have access to the Internet and to ICT systems at school. I understand that the

school will take all reasonable precautions, as outlined in the Online-Safety Policy and in line with county policy, to ensure pupils cannot access inappropriate materials, but that school cannot be held responsible, nor are liable, for any damages arising from use of the Internet in school, provided school have strictly followed policy.

I shall ensure that my child is safe online at home when on digital devices, e.g. computer, iPad, games console, mobile phone.

Signed (parent): .....

'Pupils should have an entitlement to safe Internet access at all times'

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the Internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will ensure that pupils have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement:
I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

I understand that my school will monitor my use of ICT.
I will be aware of 'stranger danger' when I am online.
I will not give any personal information about myself or others when I am online (this could include names, addresses, email addresses, telephone numbers, age etc.)
I will not send pictures of myself, of any kind, to anyone, unless it is directly supervised by an adult and is part of a planned activity to do with school e.g. educational links with another school.
I will tell an adult in school if anyone tries to talk to me online.
I will tell an adult immediately if I see anything unpleasant that makes me feel uncomfortable on the Internet, and I will lower the laptop lid immediately or turn off the monitor.
When given a username and a password I will keep it safe and to myself. I will not share it will anyone.

I will respect others' work and will not view, copy, remove or otherwise change any other users' files, without the owners' permission.
I will be polite, respectful and responsible when I communicate with others; I will not use strong, aggressive, unkind or bad language.
I will not take or show images of anyone without their permission.
I will not write, post or send anything nasty about anyone at our school. (This includes, emails, social networks and any form of mobile communication e.g. text messages – this includes doing any of these things outside school).

I will only use school devices for my school work, unless I have been given permission to use my own by a teacher.
I will not bring any personal devices in to school unless I have been given permission by a teacher. If I bring a phone in to school I will not use it and I will store it in the teacher's desk until the end of the day. I understand that if it is found in school it will be confiscated and my parents will be asked to come to collect it.
I will not try to download or upload anything from the internet without permission.
I will not use any social media at school.
I will only use a computer or device when I have been told to or if I have asked an adult's permission.
I will ask permission to bring a USB memory stick into school and I will virus scan the memory stick before copying over any files.
I will only visit websites that I have been told are safe. If I accidently come across any inappropriate websites or content on the Internet, I will immediately tell an adult and will not show anyone else but them. I will also turn off the monitor/close the lid.
I will only search for information that I have been told to by my teacher.

- I understand that I am responsible for my actions, both in and out of school.
- I understand that the school also has the right to take action against me if I break any of the above rules, or if I take part in cyberbullying.
- I understand that if I break any of the above rules then I am breaking the Online-Safety Agreement and I may be banned from the independent use of technology in school.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Name: Class:

Signed | | Date: | |

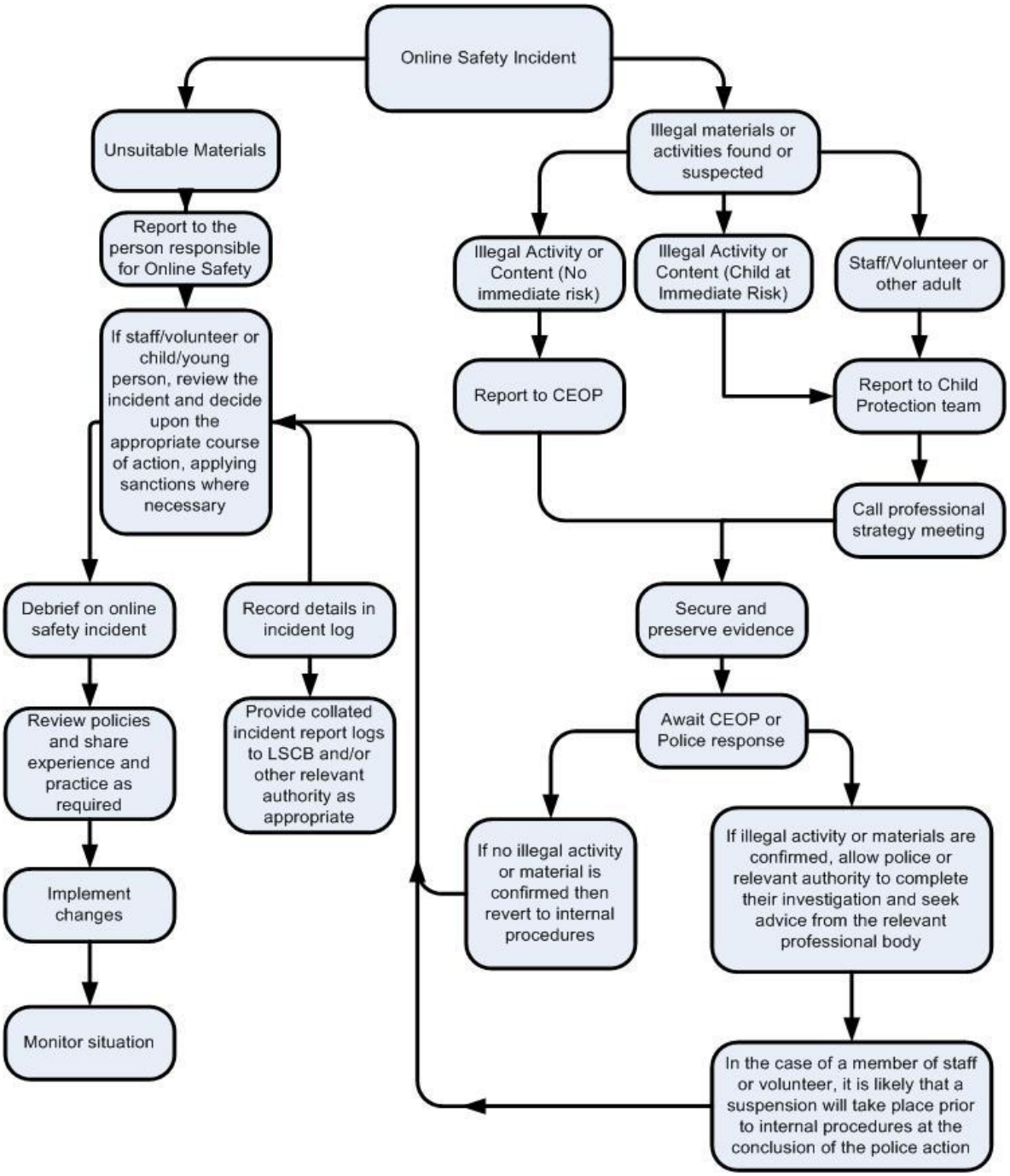
Permission Form

As the parent/carer of the above pupil, I give permission for my son / daughter to have access to the Internet and to ICT systems at school. I shall ensure that my child is safe online at home when on digital devices, e.g. computer, iPad, games console, mobile phone.

Name (parent) | | Signed: | |

Online-Safety Lead: Sue Kennedy

- takes day-to-day responsibility for online-safety issues and has a leading role in establishing and reviewing the school online-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online-safety incident taking place
- provides regular training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online-safety incidents and creates a log of incidents to inform future online-safety developments
- meets regularly with Online-safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings and committee of Governors



reports regularly to Senior Leadership Team

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 children 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 of Local Authority 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
- 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 and possibly the police, and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Informative /Useful Online Safety Websites

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

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/

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	
	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 / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. 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	
On-line gaming (educational)			X			
On-line gaming (non-educational)			X			
On-line gambling					X	
On-line shopping / commerce			X			
File sharing					X	
Use of social media					X	
Use of messaging apps					X	

Use of video broadcasting e.g. Youtube			x		

Incident Checklist	Refer to class teacher / tutor	Refer	Refer to Headteacher	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 e.g. detention or exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).									
Unauthorised use of non-educational sites during lessons									
Unauthorised use of mobile phone / digital camera / other mobile device									
Unauthorised use of social media / messaging apps / personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school network by sharing username and passwords									
Attempting to access or accessing the school network, using another pupil's account									
Attempting to access or accessing the school network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or twitter message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions									
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's filtering system									
Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									

Name: _____

Date: _____

Online-safety Lead: _____

Reporting Log Group	Signature								
	Incident Reported by								
	Action taken	By whom?								
		What?								
	Incident								
	Time								
	Date								