Howitt Primary Community School

Online Safety Policy

March 2018

Agreed by Governing Board on........................... (Date)

Signed.. (Chair)

To be reviewed...

Howitt Primary Community School
Online Safety Policy
March 2018

Scope of the Policy

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

This policy needs to be read in conjunction with;

Staff (and Volunteer) Computing Acceptable Use Policy Agreement

Pupil's Computing Acceptable Use Policy Agreement

Child Protection and Safeguarding Policy

Code of Conduct and Safer Working Practices

PSHE and RSE Policies

Tackling Extremism and Radicalisation Policy

Behaviour Policy

Anti-bullying Policy

Confidential Reporting Policy

Acceptable Use of Social Media Policy

Data Protection Policy

Roles and Responsibilities

Governors

At Howitt Primary Community School, the governing board is responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

Louise Lacey is the governor responsible for Online Safety.

The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinators
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governing Board meetings

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 Co-ordinators.
- The Headteacher and a member of the Senior Leadership 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 –Appendix 1).
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Coordinators 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 and Senior Leaders 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

Online Safety Co-ordinators are Dan Sinclair, Sharon Clarke and Chris Clarke. They will:

- lead the Online Safety Group
- take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policies / documents

- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provide training and advice for staff
- liaise with the Local Authority
- liaise with school technical staff
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- meet regularly with Online Safety Govern*or* to discuss current issues, review incident logs and filtering / change control logs
- attend relevant meetings

Technical staff is Ian Kerry

He is responsible for ensuring that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack
- Howitt Primary Community School meets required online safety technical requirements and any Local Authority / other relevant body Online Safety Policy or Guidance that may apply
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- he keeps up to date with online safety technical information in order to effectively carry out his online safety role and to inform and update others as relevant
- the use of the network, internet, remote access and emails are regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher and Online Safety Coordinators for investigation.
- that monitoring software and systems are implemented and updated as agreed in school policies

Teaching and Classroom based Staff.

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy Agreement
- pupils report any suspected misuse or problem to the Headteacher, Senior Leaders or Online Safety Coordinators for investigation and carry out appropriate actions or sanctions.
- all digital communications with pupils, parents and carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and Pupil Acceptable Use Policy Agreement
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- pupils monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned 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

Designated Safeguarding Leads

Designated Safeguarding Leads are trained in Online Safety issues and are aware of the potential for serious child protection and safeguarding issues arising from:

- sharing of personal data
- access to illegal or inappropriate materials
- inappropriate on-line contact with adults including strangers
- potential or actual incidents of grooming
- cyber-bullying

Online Safety Group

Members of the Online Safety Group will assist the Online Safety Co-ordinators with:

- the production, review and monitoring of the school Online Safety Policy and documents
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network, internet and incident logs
- consulting stakeholders – including parents, carers and the pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils:

- are responsible for using Howitt Primary Community School digital technology systems in accordance with the Pupil Acceptable Use Policy Agreement
- 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 and use of images and on cyber-bullying
- should understand the importance of adopting good online safety practice when using digital technologies out of school

Parents / Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Howitt Primary Community School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, workshops, letters, website and information about national or local online safety campaigns and 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

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

- a planned online safety curriculum is provided as part of Computing, PHSE and other lessons and is regularly revisited
- key online safety messages are reinforced as part of a planned programme of assemblies and extra-curricular events
- pupils are taught in all lessons to be critically aware of the materials or content they access on-line and be guided to validate the accuracy of information.
- pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- pupils are supported in a safe environment for debating controversial issues and helped 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 Policy and encouraged to adopt safe and responsible use both within and outside school
- staff act as good role models in their use of digital technologies, the internet and mobile devices
- where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
- it is accepted that from time to time, for good educational reasons, pupils 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.

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 of the children's on-line 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.

Howitt Primary Community School will therefore seek to provide information and awareness to parents and carers through:

- curriculum activities
- letters, newsletters, school website
- parents /Carers evenings, workshops and 'open book' evening
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites and publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers
- NSPCC leaflets, Digital Parenting magazines and other literature

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- all new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements

The Governing Board will take part in online safety training awareness sessions, with particular importance for those who are members of any subcommittee group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL)
- participation in school information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

Howitt Primary Community School is 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 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 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.
- all users will be provided with a username and secure password. Users are responsible for the security of their username and password and will need to change it regularly
- the "master / administrator" passwords for the school Computing system, used by the Network Manager must also be available to the Headteacher and other nominated senior leaders and kept in a secure place.
- **Ian Kerry** 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 by Sharon Clarke every week. School laptops that have been used at home are also checked.
- internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet
- staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy Agreements
- an appropriate system is in place for users to report any technical or security breach
- appropriate security measures are in place 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. All memory sticks are encrypted

Mobile Technologies (including BYOD - Bring Your Own Devices/BYOT - Bring Your Own Tablets)

Mobile technology devices may be school owned or provided or personally owned and might include: smartphone, tablet, notebook, laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile or personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy Agreement and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

- Howitt Primary Community School's Acceptable Use Policy Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies

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 the pupils and the staff.

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers is 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 Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents /

carers comment on any activities involving other *pupils* in the digital / video images. Parents do sign a school form at concerts and school events agreeing to follow the school policy on taking any photos or videos at such events.

- 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. School cameras and Ipads will be taken on trips.
- Care is 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 into disrepute. This will include the school logo not being visible if there are any Safeguarding issues.
- 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 pupil and parents or carers.

Data Protection

Howitt Primary Community School will follow the Data Protection Policy.

Staff must ensure that they:

- take care at all times 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.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies, the school considers the following as good practice:

- the official school email service is safe and secure and is monitored.
- users must immediately report any receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE (Virtual Learning Environment) etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

(Refer to Social Media Policy)

Howitt Primary Community School has a duty of care to provide a safe learning environment for pupils and staff.   Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise the risk of harm to pupils, staff and the school through:

- ensuring that personal information is not published
- training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk

School staff should ensure that:

- no reference should be made in social media to pupils, parents / carers or school staff
- they do not engage in online discussion on personal matters relating to members of Howitt Primary Community School.
- personal opinions should not be attributed to Howitt Primary Community School or local authority
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- a process for approval by senior leaders
- clear processes for the administration and monitoring of these accounts
  (Refer to Acceptable Use Policy Agreement for staff)

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- Howitt Primary Community School will effectively respond to social media comments made by others if appropriate.

Signed ………………………………………………………….

Date………………………………………………………….

To be reviewed ………………………………………….

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.

Online Safety Incident

Unsuitable Materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Review policies and share experience and practice as required

Implement changes

Monitor situation

Record details in incident log

Provide collated incident report logs to LSCB and/or other relevant authority as appropriate

Illegal materials or activities found or suspected

Illegal Activity or Content (No immediate risk)

Illegal Activity or Content (Child at Immediate Risk)

Staff/Volunteer or other adult

Report to CEOP

Report to Child Protection team

Call professional strategy meeting

Secure and preserve evidence

Await CEOP or Police response

If no illegal activity or material is confirmed then revert to internal procedures

If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action