WASHACRE PRIMARY SCHOOL

ONLINE SAFETY POLICY

Written July 17
J Haunch, A Briffa, K Walsh

Development / Monitoring / Review of this Policy

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

- *Miss Haunch, Headteacher and Safeguarding Lead Officer*
- *Mrs Briffa, Computing Subject Lead and Safeguarding Officer*
- *Mrs Walsh, School Governor*

Consultation with the staff has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This Online policy was approved by the *Governing Body on*	*28.12.16 and reviewed by a working party in July 17.*
The implementation of this Online policy will be monitored by the Senior Leadership Team and Computing Subject Lead.	*Senior Leadership Team*
Monitoring will take place at regular intervals:	
The *Governing Body Curriculum Sub-Committee* will receive a report on the implementation of the Online policy generated by the monitoring group (which will include anonymous details of Online incidents) at regular intervals:	*Once per year*
The Online 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 or incidents that have taken place. The next anticipated review date will be:	*September 2018*
Should serious Online incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager, LA Safeguarding Officer, LADO, HR, Police*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Surveys / questionnaires of*
- *pupils*
- parents / carers
- *staff*

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers 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 cyber-bullying, or other online 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. 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 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.*

Governing Board:

Governors are responsible for the approval of the Online Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governing Body Curriculum Sub Committee* receiving regular information about online incidents and monitoring reports. A member of the *Governing Body* has taken on the role of *Online Governor* (Ron Bell)
The role of the Online *Governor* will include:

- *regular meetings with the Online Co-ordinator*
- *regular monitoring of online incident logs*
- *reporting to relevant Governors*

Head teacher and Senior Leaders:

The *Head teacher* has a duty of care for ensuring the safety (including Online) of members of the school community, though the day to day responsibility for Online will be delegated to the *Online Co-ordinator.*

- The Head teacher and 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 allegation being made against a member of staff. (See flow chart on dealing with Online incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority HR / other relevant body* disciplinary procedures).

- *The Head teacher and Senior Leaders are responsible for ensuring that the Online Coordinator and other relevant staff receive suitable training to enable them to carry out their Online roles and to train other colleagues, as relevant.*

- *The Head teacher 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 monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.* Additional PPA time will be provided to ensure rigorous monitoring occurs.

- *The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the Online Co-ordinator / Officer.*

Computing / Online Safety subject leader:

The headteacher with the support of the computing lead:

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

In the case of any reported incidents the headteacher will seek the advice of HR and other agencies such as the LADO or Safeguarding team.

Network Manager / Technical staff from Bolton SICT:

The *Technical Staff from Bolton IT services in liaison with the Computing* lead are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online technical requirements and any Local Authority Guidance that may apply.
- that 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
- that they keep up to date with online technical information in order to effectively carry out their Online role and to inform and update others as relevant
- that the use of the network, internet, Virtual Learning Environment, remote access, email is regularly monitored in order that any misuse or attempted misuse can be reported to the Head teacher or Computing subject leader for investigation
- that monitoring software and systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online matters and of the current *school*

Online policy and practices

- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the *Headteacher* for investigation
- all digital communications with students, pupils, parents, carers should be on a professional level *and only carried out using official school systems*
- Online issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online and acceptable use policies
- they 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*

Child Protection / Designated Safeguarding Leads (JH/CM/GY/VB/LT)

Are be trained in Online issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

These are child protection issues, not technical issues, simply which the technology provides additional means for child protection issues to develop.

Pupils

- are responsible for using the *school* digital technology systems in accordance with the User Policy

- 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 cyber-bullying.
- should understand the importance of adopting good online practice when using digital technologies out of school and realise that the *school's* Online Policy covers their actions out of school, if related to their membership of the school

Parents and 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. The *school* will take every opportunity to help parents understand these issues through *parents' and carers evenings, newsletters, letters, website. VLE and information about national / local online safety campaigns and literature.* Parents and carers will be encouraged to support the *school* in promoting good online 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 / VLE and on-line student / pupil records.

Community Users

Community Users who access school systems / website / VLE as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems. (The Community Users Acceptable Use Policy Template can be found in the appendices.

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 therefore an essential part of the school's online provision. Children and young people need the help and support of the school to recognise and avoid online risks and build their resilience.

Online safety is be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The Online safety curriculum is be broad, relevant and provide 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 / other lessons and is regularly revisited

- Key Online safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- pupils are taught in all lessons to be critically aware of the materials and 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 helped to understand the need for the Acceptable Use Policy (AUPs) 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*
- *in lessons where internet use is pre-planned, pupils are 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 are vigilant in monitoring the content of the websites visited*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, will be auditable, with clear reasons for the need.*

Education – parents / carers

Many parents and carers have only a limited understanding of the online risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-

line behaviours. Parents and carers 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 and parents and carers workshops*
- *Letters, newsletters, web site, VLE*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications e.g.*

www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers CEOPS,

Education – The Wider Community

The school will provide opportunities for members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:
Providing family learning courses in use of new digital technologies, digital literacy and
Online messages targeted towards grandparents and other relatives as well as parents.

The school website will provide online information for the wider community

Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their online safety provision

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 programme of formal and informal online safety training is available to staff. This is regularly updated and reinforced. An audit of the online training needs of all staff is carried out regularly.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.
- *Safeguarding and Computing leads receive regular updates through attendance at external training events (e.g. from / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This Online safety policy and its updates will be presented to and discussed by staff in staff and team meetings and on INSET days.*
- *Safeguarding and Computing lead (or other nominated person) will provide advice, Guidance, training to individuals as required.*

Training – Governors

Governors should take part in online training and awareness sessions, with particular importance for those who are members of any subcommittee or group involved in technology, Online, health and safety, child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

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 responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (these may are outlined in Local Authority / other relevant body policy and guidance)
- 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 / academy technical systems and devices.
- All users in KS2 will be provided with a username and secure password by *the computing lead who will keep an up to date record of users and their usernames.* Users are responsible for the security of their username and password *and will be required to change their password every year*.
- The " administrator" passwords for the school ICT system, used by the Network Manager (or other person) will be available to the *Headteacher and Business Manager* and kept in a secure place
- The Business Manager 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
- *The school has provided enhanced user-level filtering*
- *School technical 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 Agreement*
- *An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed). Concerns are reported to the Computing Lead and the Headteacher*
- 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.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of Online considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

The school has a set of clear expectations and responsibilities for all users
The school adheres to the Data Protection Act principles
All users are provided with and accept the Acceptable Use Agreement
All network systems are secure and access for users is differentiated
Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
All users will use their username and password and keep this safe
Mandatory training is undertaken for all staff
Pupils receive training and guidance on the use of personal devices
Regular audits and monitoring of usage will take place to ensure compliance
Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
Any user leaving the school will follow the process outlined within the BYOD policy

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 will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- 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 in not covered by the Data Protection Act). 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 *students / pupils* in the digital / video images. Where parents / carers have not permitted images of their children to be taken, staff will ask all parents to refrain from taking images of the event involving that child.
- *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 students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school 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.*
- *Written permission from parents or carers will be obtained before photographs of* students/pupils are published on the school website
- *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 Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. A School Personal Data template is available in the appendices to this documentThe school / academy must ensure that:
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.
Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
It has a Data Protection
It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs) Risk assessments are carried out
It has clear and understood arrangements for the security, storage and transfer of personal data
Data subjects have rights of access and there are clear procedures for this to be obtained
There are clear and understood policies and routines for the deletion and disposal of data
There is a policy for reporting, logging, managing and recovering from information risk incidents
There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- 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.

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
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

This is an area of rapidly developing technologies and uses.
A wide range of rapidly developing communications technologies has the potential to enhance learning.
The following table shows how our school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

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

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	√							√
Use of mobile phones in lessons				√				√
Use of mobile phones in social time		√						√
Taking photos on mobile phones or personal cameras				√				√
Use of other mobile devices belonging to school			√				√	
Use of personal email addresses in school, or on school network				√				√
Use of school email for personal emails				√				√
Use of messaging apps			√					√
Use of school social media			√					√
Use of school blogs	√				√			

- The official *school* email service may be regarded as safe and secure and is monitored. Users are that email communications are monitored.
- Users must immediately report, to the headteacher – the 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, chat, VLE 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.*
- *Whole class / group email addresses may be used at KS1, while pupils at KS2 will be provided with individual school email addresses for educational use.*
- *Pupils are taught about Online issues, such as the risks attached to the sharing of personal details. They are taught strategies to deal with inappropriate communications and are reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information is not posted on the school website and only official email addresses are used to identify members of staff.*

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. While, Ofsted's Online framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority liable to the injured party. Reasonable steps to prevent predictable harm are in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:
Training to include: 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 (Facebook will have images of pupils but no personal detaila)
Staff must not engage in online discussion on personal matters relating to members of the school community personal opinions should not be attributed to the *school* or local authority
Security settings on personal social media profiles are checked to minimise risk of loss of personal information.

The *school's* use of social media for professional purposes will be checked regularly by the Computing Lead to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

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 school or outside 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	
	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	
	Facebook friending a pupil or parents/carers of pupils at school				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 (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) using Platforms which are not approved by school					X	

On-line gaming (non educational)				X	
On-line gambling				X	
On-line shopping / commerce		X			
File sharing		X			
Use of social media, ie Washacre Facebook		X			
Use of messaging apps, ie Blog		X			
Use of video broadcasting e.g. YouTube				X	

Responding to incidents of misuse
This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

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 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:

If there are any concerns these must be reported to the headteacher and the computing lead.

With support from HR and IT the headteacher will conduct the investigation procedure using a designated computer that will not be used by children or staff and if necessary can be taken off site by the police should the need arise. The same computer will be used for the duration of the procedure.
During the investigation the sites and content visited are closely monitored and recorded (to provide further protection). 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 headteacher with the support of HR 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 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.

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:

Pupils

Incidents:	Refer to class teacher	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering	Inform parents / carers	Removal of network , internet access rights	Warning	Further sanction e.g. 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	X	X	X	X	
Unauthorised use of non-educational sites during lessons	X	X		X	X	X	X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X			X		X	
Unauthorised use of social media / messaging apps / personal email	X	X			X	X	X	
Unauthorised downloading or uploading of files	X	X			X		X	
Allowing others to access school network by sharing username and passwords	X	X			X		X	
Attempting to access or accessing the school, using another pupil's account	X	X			X		X	
Attempting to access or accessing the school network, using the account of a member of staff	X	X			X		X	

Deliberately corrupting or destroying the data of other users	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
Continued infringements of the above, following previous warnings or sanctions	X	X			X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X			
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X

Staff **Actions / Sanctions**

Incidents:	Refer to Computing Lead	Refer to Head teacher	Refer to Local Authority Designated Officer & HR	Refer to Police	Refer to Technical Support Staff for action	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	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X	X				X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X				X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X				X		
Deliberate actions to breach data protection or network security rules	X	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	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	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	X	X	X	X	X	X	X	X
Actions which could compromise the staff member's professional standing								

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X	X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X				X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X	X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	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	X	X