



Halfpenny Lane J, I & N

Online Safety Policy

November 2018

Contents

Introduction.....	3
Schedule for Development/Monitoring/Review	3
Aims	4
Roles and Responsibilities	4
Governors	4
Head of School and Senior Leaders	4
Online Safety Officer.....	5
Network Manager / Technical Staff.....	5
Staff	6
Designated Safeguarding Lead	6
Pupils	7
Parents and Carers.....	7
Policy Statements	7
Education of Pupils	7
Education of Parents/Carers.....	8
Education and Training for Staff and Volunteers.....	9
Training for Governors.....	9
Technical – infrastructure / equipment, filtering and monitoring.....	9
Use of digital and video images.....	11
Data Protection.....	Error! Bookmark not defined.
Communications.....	12
Unsuitable / inappropriate activities	13
Responding to incidents of misuse	14
Illegal Incidents	15
Other Incidents	15
Record of reviewing devices / internet sites (responding to incidents of misuse).....	17
Name and location of computer used for review (for web sites).....	17
School Actions and Sanctions	17

Introduction

Using the internet is becoming an increasingly large part of everyday life for many people and has huge power which can be harnessed for fantastic learning opportunities. However, this power can also be misused, both intentionally and unintentionally.

The Education and Inspections Act 2006 empowers Headteachers to such an 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 Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the cases of both acts, action can only be taken over issues covered by the published Behaviour Policy.

This policy provides guidance on how our school uses the internet and social media, and the procedures for doing so. It applies to all members of the school community who have access to and are users of school ICT systems, both in and out of the school. It also outlines how we expect the staff, volunteers and children of Halfpenny Lane School to behave online. It should be read in conjunction with the Safeguarding Policy, the Behaviour Policy and Code of Conduct for Staff.

The policy has been drawn up as a result of staff discussion and has full agreement of the Governing Body. The implementation of this policy is the responsibility of all the teaching staff.

Schedule for Development/Monitoring/Review

The implementation of this Online Safety policy will be monitored by:	Lynda Hewes – Online Safety Officer SLT
Monitoring will take place at regular intervals:	Termly
The Governing Board will receive a report on the implementation of the Online Safety Policy at regular intervals	At least once per year
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be	June 2019
Should serious online safety incidents take place, the following external persons/ agencies should be informed:	

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Surveys/questionnaires of
 - Pupils
 - Parents and carers
 - Staff

Aims

The aims of our online safety policy are:

- **To protect**
 - *Children* - It is the duty of the school to ensure that every child in its care is safe, and the same principles that apply to the school's physical world apply to its 'virtual' or digital world.
 - *Staff* and all members of the school community who have access to the school's IT systems both in and out of the school.
 - *Data* – In accordance with...
- **To provide**
 - *Advice and guidance* on how to minimise risks.
 - *Procedures* to follow when responding to incidents
 - *Information* for staff, volunteers, parents, governors and any other stakeholders of the school around all aspects of how Online Safety is taught and managed at Halfpenny Lane School.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Halfpenny Lane School.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.

Head of School and Senior Leaders

The Head of School 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:

Lynda Hewes – Online Safety Officer

James Parkinson - Designated Safeguarding Lead

The Head of School and (at least) another 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.

The Head of School and SLT are responsible for ensuring that the Online Safety Officer 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 Head of School and SLT 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 those colleagues who take on important monitoring roles.

The SLT will receive regular monitoring reports from the Online Safety Officer.

Online Safety Officer

The Online Safety Officer:

- 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 training and advice for staff.
- Liaises with the Local Authority/relevant body.
- Liaises with school technical staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Attends relevant meetings of the Governing Board.
- Reports regularly to SLT.
- Maps and reviews the online safety curricular provision – ensuring relevance, breadth and progression.
- Consults with stakeholders, including parents/carers and pupils, about the online safety provision.
- Monitors improvement actions.

Network Manager / Technical Staff

The network is managed by Alamo Business Systems. It is the responsibility of the school to ensure that they carry out all the online safety measures that would otherwise be the responsibility of the school technical staff as outlined below.

Alamo should ensure:

- That the school's infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any Pontefract Academies Trust Online Safety Policy / 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 safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network, internet and email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of School or the Online Safety Officer for investigation / action / sanction.
- That monitoring software and systems are implemented and updated as agreed in the school policies.

Staff

All staff members 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.

All staff should have signed, and be familiar with, the Staff Acceptable Use Policy and be aware that this applies to all school IT equipment, whether it is used at school or at home.

Any suspected misuse or problem should be reported (by any staff member) to the Head of School or the Online Safety Officer.

All digital communications with pupils / parents and carers should be on a professional level and only carried out using official school systems.

Staff are responsible for ensuring that online safety issues are embedded into all aspects of the curriculum and other activities. This includes pupils having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

All staff members are responsible for ensuring that pupils understand and follow the Online Safety Policy by monitoring the use of digital technologies, mobile devices, cameras etc in lessons and other school activities, and by implementing 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. Staff members are responsible for ensuring that processes are in place with their class for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead

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

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

It is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop.

Pupils

Pupils are responsible for using the school digital technology systems. They should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Pupils need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Pupils 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.

Pupils should understand the importance of adopting good online safety practice when using digital technologies out of schools and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and Carers

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

- digital and video images taken at school events
- their children's personal devices in the school

Policy Statements

Education of 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 safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- A planned online safety curriculum, provided as part of Computing / PHSE / other lessons which will be regularly revisited

- Key online safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. There are additional duties for schools under the Counter Terrorism and Securities Act 2015 which require them to ensure that children are safe from terrorist and extremist material on the internet.
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that Alamo 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 of Parents/Carers

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

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

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day

- Reference to the relevant web sites / publications e.g. swgfl.org.uk
www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>

Education and Training for Staff and 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. An audit of the online safety training needs of all staff will be carried out regularly.
- 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.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Officer will receive regular updates through attendance at external training events 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 / team meetings / INSET days.
- The Online Safety Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Training for Governors

Governors should 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.
- Participation in school / academy training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (these may be outlined in Local Authority / Academy Group / 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 technical systems and devices.
- All users will be provided with a username and secure password by Alamo 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 90 days. The “master / administrator” passwords for the school / academy ICT system, used by the Network Manager (or other person) must also be available to the Head of School or other nominated senior leader and kept in a secure place (eg school safe)
- Alamo are 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 (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet. See Prevent Duty for more details.
- Alamo has provided differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc)
- Alamo 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.
- 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.
- An agreed policy is in place (to be described) regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.

- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place that the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices is not allowed. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

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

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school / academy 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 / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school / trust policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school / academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission

Use of messaging apps								
Use of social media								
Use of blogs								

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 / academy 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 /academy context, either because of the age of the users or the nature of those activities.

The school / academy believes that the activities referred to in the following section would be inappropriate in a school / academy context and that users, as defined below, should not engage in these activities in / or outside the school / academy when using school / academy equipment or systems. The school / academy 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,	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X

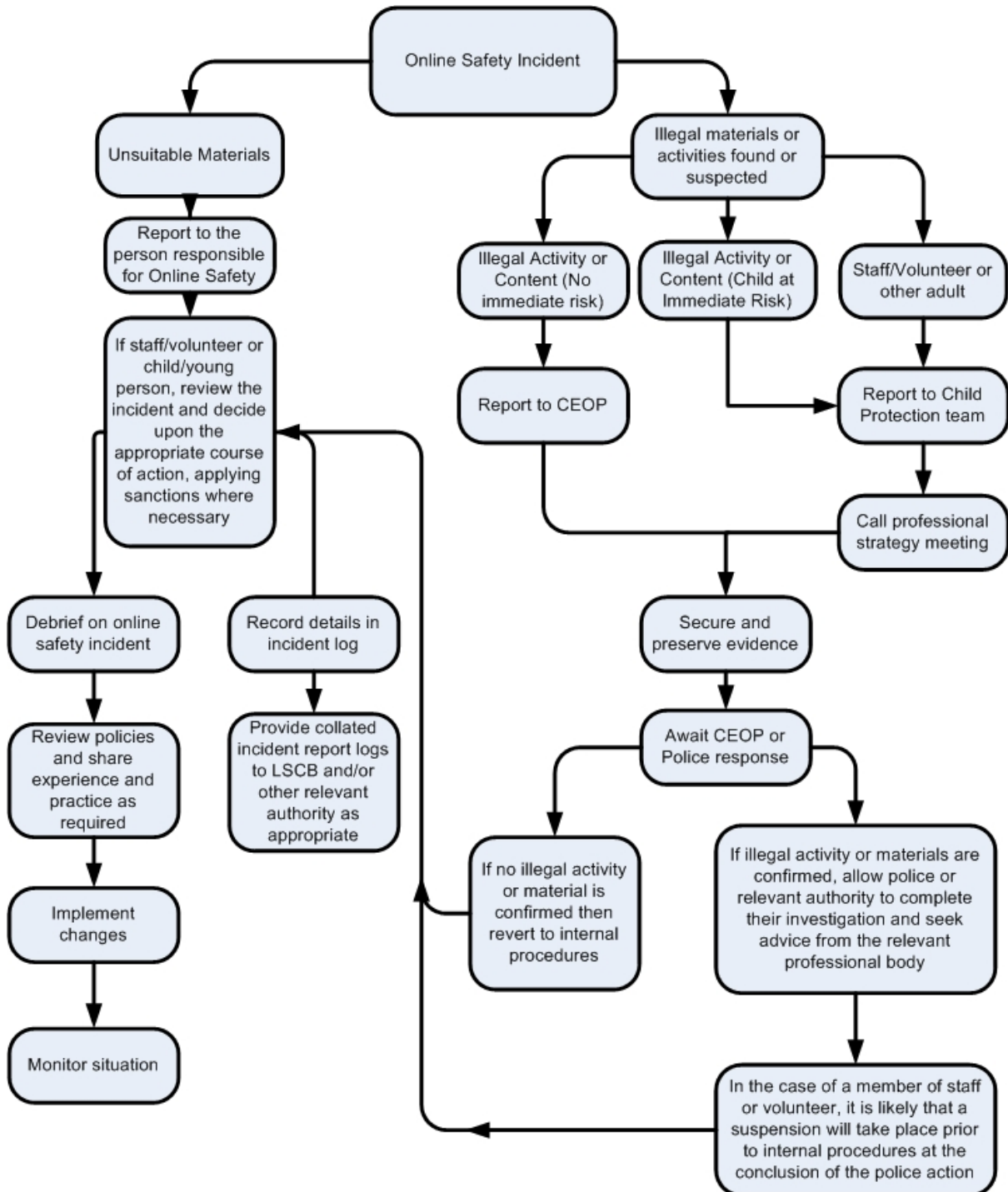
Pornography				X	
Promotion of any kind of discrimination				X	
threatening behaviour, including promotion of physical violence or mental harm				X	
Promotion of extremism or terrorism				X	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)					
On-line gaming (non-educational)					
On-line gambling					
On-line shopping / commerce					
File sharing					
Use of social media					
Use of messaging apps					
Use of video broadcasting e.g. Youtube					

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, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may

be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

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

It is important that all of the above steps are taken as they will provide an evidence trail for the school / academy and possibly the police and demonstrate that visits to

these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group:

Date:

Reason for investigation:

.....

.....

.....

Details of first reviewing person

Name:

Position:

Signature:

Details of second reviewing person

Name:

Position:

Signature:

Name and location of computer used for review (for web sites)

.....

.....

<i>Web site(s) address / device</i>	<i>Reason for concern</i>
-------------------------------------	---------------------------

Conclusion and Action proposed or taken

School Actions and Sanctions

It is more likely that the school / academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt

with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Actions / Sanctions

Students / Pupils Incidents	Refer to class teacher	Refer to Phase Leader	Refer to Head of School	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X							X	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X							
Unauthorised / inappropriate use of social media / messaging apps / personal email	X	X							
Unauthorised downloading or uploading of files	X	X	X						
Allowing others to access school / academy network by sharing username and passwords	X	X						X	X
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X								
Attempting to access or accessing the school / academy network, using the account of a member of staff	X	X	X					X	X
Corrupting or destroying the data of other users	X	X	X					X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	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 / academy into disrepute or breach the integrity of the ethos of the school	x	x	x				x	x	x
Using proxy sites or other means to subvert the school's / academy's filtering system		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
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x	x	x	x					

Actions / Sanctions

Staff Incidents

	Refer to line manager	Refer to Head of School	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x	x				
Inappropriate personal use of the internet / social media / personal email	x	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		
Deliberate actions to breach data protection or network security rules		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

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x					x	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x	x			x		X	
Actions which could compromise the staff member's professional standing		x	x			x		x	
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	x	x	x			x	x	x	
Using proxy sites or other means to subvert the school's / academy's filtering system	x	x	x				x	x	
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x	x			x	x	x
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x			x	x	x
Breaching copyright or licensing regulations	x	x	x				x	x	x
Continued infringements of the above, following previous warnings or sanctions	x	x	x				x	x	x