St Mary's CE Primary Academy - Online Safety Policy & ICT Acceptable Usage Agreement (AUA)

(Reviewed November 2018)

Rationale

As a Church School working with our local, national and international communities, ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At St Mary's Primary School, we understand the responsibility to educate our pupils on Online Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreements (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, and portable media players, etc).

Child Protection / Safeguarding Designated Person / Officer

should be trained in e-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 on-line contact with adults / strangers
- potential or actual incidents of grooming

- cyber-bullying

Roles and Responsibilities
As Online Safety is an important aspect of strategic leadership within the school the Governing Body have ultimate responsibility to ensure that the policy and practices are embedded and monitored. This responsibility is delegated to the Head. Any extra permission given by the Head must be recorded (e.g. memos, minutes from meetings) in order to be valid.

The named person (Mrs Nightingale) and ICT manager (Miss Stelfox) have the responsibility of ensuring this policy is upheld by all members of the school community and that they have been made aware of the implication this has. It is the role of these members of staff to keep abreast of current issues and guidance through organisations such as the LA, Becta, CEOP (Child Exploitation and Online Protection), Childnet and Local Authority Safeguarding Children Board.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, safeguarding policy and behaviour/pupil discipline (including the anti-bullying) policy.

Online Safety skills development for staff

- Our staff receive regular information and training on e-safety issues in the form of full staff meetings and memos.
- New staff receive information on the school's acceptable use policy as part of their induction through their staff handbooks.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas.

Communicating the school Online Safety messages

- Online Safety rules will be posted in all classrooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- Online Safety posters will be prominently displayed, especially in the ICT suite.

Online Safety in the Curriculum
ICT and online resources are increasingly used across the curriculum. We believe it is essential for Online Safety guidance to be given to the pupils on a regular and meaningful basis. Online Safety is embedded within our curriculum and we continually look for new opportunities to promote Online Safety. We regularly monitor and assess our pupils' understanding of Online Safety.

- The school provides opportunities within a range of curriculum areas and discrete ICT lessons to teach about Online Safety (in accordance with the medium term planning.)
- Educating pupils on the dangers of technologies that maybe encountered outside school may also be done informally when opportunities arise.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

Password Security
Password security is essential for staff, particularly as they are able to access and use pupil data. Staff have access to this through Administrator Rights on the NGFL network. The pupils from Year R upwards have individual logins and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

Data Security
The accessing and appropriate use of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data. Level of access is determined by the Head Teacher. Data can only be accessed and used on school computers or laptops. Staff must operate the 'screen locked' function or close down laptops or personal computers when not at their desk. Staff are aware they must not use their personal devices for accessing any school/pupil data.

Managing the Internet
The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.

- All staff must read and agree to the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- School internet access is controlled through the LA's web filtering service.
- Our school also employs some additional web filtering.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be left on (so as to record and report the specific site appropriately) and the incident reported **immediately** to the class teacher who must inform Internet Safety Leader, Miss Stelfox.
- It is the responsibility of the school, by delegation to the technical support; to ensure that Anti-virus protection (Sophos) is installed and kept up-to-date on all school machines.
- If pupils wish to bring in work on removable media it must be given to the teacher for a safety check first.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the ICT Manager.
- If there are any issues related to viruses or anti-virus software, the ICT manager should be informed through the 'Computer Problems' book held in the school office.

Managing other Web 2 technologies
Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture

and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to unmonitored social networking sites such as Facebook to pupils within school.
- There should be no communication between staff and pupils through social networking sites such as Facebook.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school.
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the LA Learning Platform or other systems approved by the Head Teacher.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. The school does not permit a member of staff to contact a pupil or parent/ carer using their personal device, unless it is a matter of emergency.
- Pupils are not allowed to bring personal mobile devices/phones to school unless this is for educational purposes set by the teacher (even then, stict monitoring and controlled usage will only be permitted).
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or internationally. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'.

- The school gives all staff their own email (I mail) account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- The following pupils have their own individual school issued accounts; R – Year 6. All other children use a class/ group email address.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arranging to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the ICT manager if they receive an offensive e-mail.
- Pupils are introduced to email as part of the ICT Curriculum from Year 3.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on school trips.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of others, this includes when on school trips. With the consent of the class teacher, pupils are permitted to take digital cameras from school to record images and can download these images on the school network.

Publishing pupil's images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' full names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.

Before posting pupils' work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Storage of Images

Images/ films of children are stored on the school's network.

- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head Teacher

- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform.
- Teaching Staff have the responsibility of deleting the images when they are no longer required, or when the pupil has left the school.

Misuse and Infringements

Complaints

- Complaints relating to Online Safety should be made to the ICT manager or Head Teacher.
- All incidents will be logged and followed up.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and must be reported to Mrs Nightingale (Safeguarding Officer).
- Pupils and parents will be informed of the complaints procedure.

Inappropriate material (see ICT Acceptable Use Agreement)

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Online Safety co-ordinators.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT manager, depending on the seriousness of the offence; investigation by the Head Teacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' Online Safety rules.
However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.
Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online Safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting Online Safety both in and outside of school. We regularly consult and discuss Online Safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to Online Safety where appropriate in the form of;
    - Information sessions
    - Posters
    - Learning Platform postings/links to further information
    - Newsletter items
- Parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupil.

- Parents/carers are expected to reinforce the guidance from school when using technologies at home. The school will not be responsible for communications between pupils' outside school through social networking sites.

ICT Acceptable Use Agreement (AUA)

(Reviewed November 2018)

POLICY STATEMENT

The Governing Body recognises the use of ICT as an important resource for teaching, learning and personal development. It actively encourages staff to take full advantage of the potential for ICT to enhance development in all areas of the curriculum and school administration. It is also recognised by the Governing Body that along with these benefits there are also responsibilities, especially for ensuring that children are protected from contact with inappropriate materials.

In addition to their normal access to the school's ICT systems for work-related purposes, the Governing Body permits staff limited reasonable personal use of ICT equipment and e-mail and internet facilities during their own time subject to such use:

1. *not depriving pupils of the use of the equipment*

   and/or

2. *not interfering with the proper performance of the staff member's duties*

Whilst the school's ICT systems may be used for both work-related and for personal reasons the Governing Body expects use of this equipment for any purpose to be appropriate, courteous and consistent with the expectations of the Governing Body at all times and must never compromise the **high standards of Safeguarding** expected by all members of the staff.

The use of computer equipment, including laptop computers, which is on loan to staff by the school for their personal use at home is covered under this policy. Staff who have equipment on loan are responsible for its safekeeping and for ensuring that it is used in compliance with this policy.

GUIDANCE ON THE USE OF SCHOOL ICT FACILITIES

Whilst it is not possible to cover all eventualities, the following information is published as guidance for staff on the expectations of the Governing Body. Any non-conformance to this policy or operation outside statutory legal compliance may be grounds for disciplinary action being taken up to and including disciplinary action

Further guidance on the responsible use of ICT facilities are contained in the Council document *"Internet Access Policy for Schools"*.

E-mail and Internet usage

The following uses of the school's ICT system are prohibited and may in certain circumstances amount to gross misconduct and could result in dismissal:

1. *to gain access to, and/or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that would tend to deprave or corrupt those likely to read or see it*

2. *to gain access to, and/or for the publication and distribution of material promoting racial hatred*

3. *for the purpose of bullying or harassment, or for or in connection with discrimination or denigration on the grounds of gender, race, disability or sexual orientation*

4. *for the publication and/or distribution of libellous statements or material which defames or degrades others*

5. *for the publication and distribution of personal data without either consent or justification*

6. *where the content of the e-mail correspondence is unlawful or in pursuance of an unlawful activity, including unlawful discrimination*

7. *to participate in on-line gambling*

8. *where the use infringes copyright law*

9. *to gain unauthorised access to internal or external computer systems (commonly known as hacking)*

10. *to enable or assist others to breach the Governors' expectations as set out in this policy*

Additionally, the following uses of school ICT facilities are not permitted and could lead to disciplinary action being taken:

1. *for participation in "chain" e-mail correspondence*

2. *in pursuance of personal business or financial interests, or political activities (excluding the legitimate activities of recognised trade union representatives)*

3. *to access ICT facilities using another person's password, or to post anonymous messages or forge e-mail messages using another person's identity.*

Use of School ICT Equipment

Users of school ICT equipment:

1. *must not share and must treat as confidential any passwords provided to allow access to ICT equipment and/or beyond firewall protection boundaries*

2. *must report any known breach of password confidentiality to the Headteacher or nominated ICT Co-ordinator as soon as possible*

3. *must report known breaches of this policy, including any inappropriate images or other material which may be discovered on the school's ICT systems*

4. *must not install software on the school's ICT systems, including freeware and shareware, unless authorised by the school's ICT Co-ordinator*

5. *must comply with any ICT security procedures governing the use of systems in the school, including anti-virus measures*

Regulation of Investigatory Powers Act 2000

Ancillary to their provision ICT facilities the Governing Body asserts the employer's right to monitor and inspect the use by staff of any computer or telephonic communications systems where there are grounds for suspecting that such facilities are being, or may have been, misused.

Unsuitable / inappropriate activities

Some internet activity eg 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 eg 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:

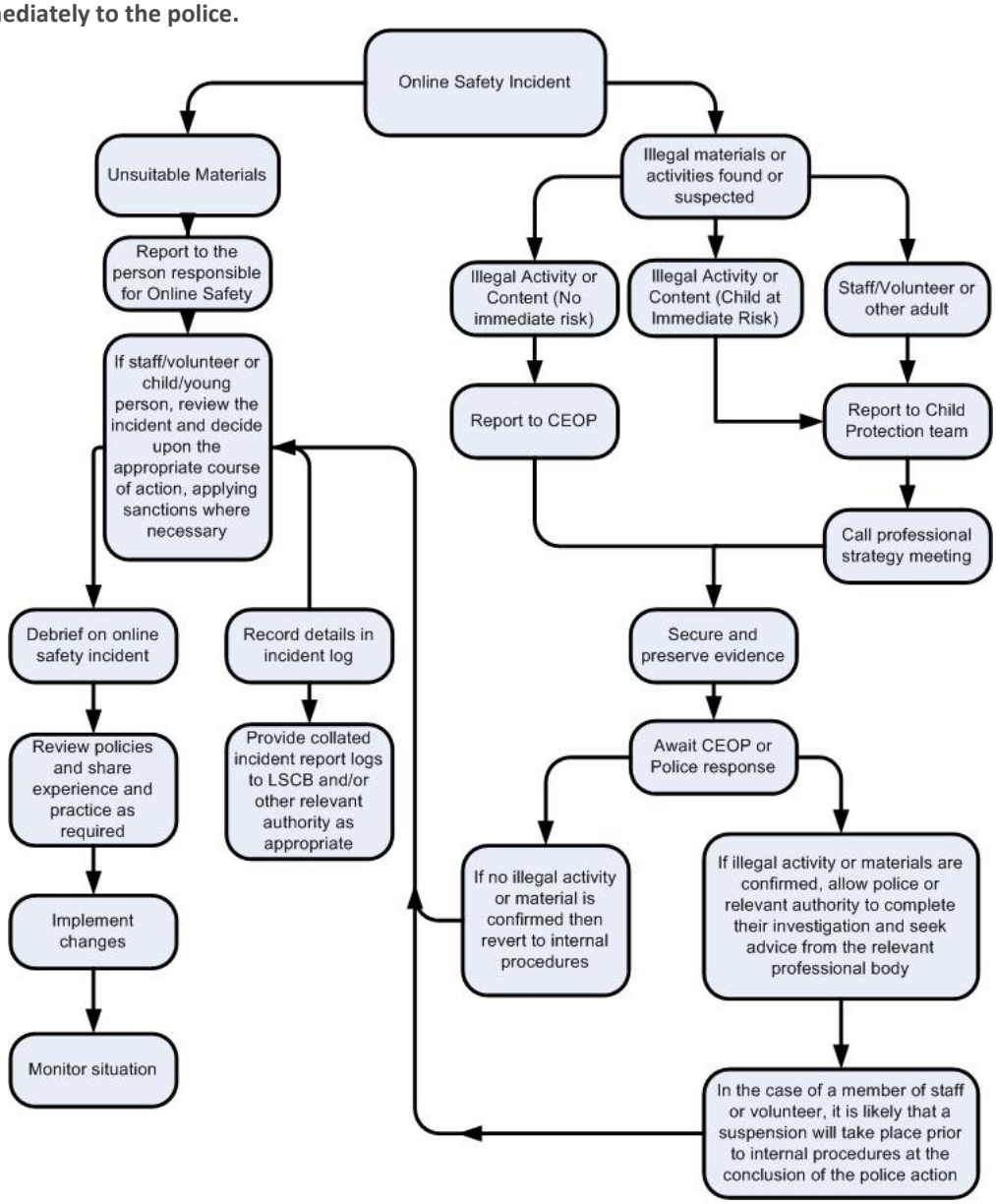
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child 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	
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)				X		
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce					X	
File sharing				X		
Use of social media					X	
Use of messaging apps					X	
Use of video broadcasting eg 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, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / academy 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:
    - 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 / academy* 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 / Academy Actions & 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:

Students / Pupils

Incidents:	Refer to class teacher / tutor	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	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	
Unauthorised downloading or uploading of files	x	x			x		x	
Attempting to access or accessing the school / academy network, using another student's / pupil's account	x	x			x		x	
Attempting to access or accessing the school / academy network, using the account of a member of staff	x	x			x		x	
Corrupting or destroying the data of other users	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
Continued infringements of the above, following previous warnings or sanctions	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		x
Using proxy sites or other means to subvert the school's / academy's filtering system	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
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x	x	x	x	x	x		x

Staff

Incidents:	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X				
Inappropriate personal use of the internet / social media / personal email	x	x		x	x		
Unauthorised downloading or uploading of files	x	x	x	x	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	x	x	x	x
Careless use of personal data eg holding or transferring data in an insecure manner	x	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

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x		x	x		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	x	x	x	x	x	x	x
Actions which could compromise the staff member's professional standing	x	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 / academy	x	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	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
Breaching copyright or licensing regulations	x			x	x		
Continued infringements of the above, following previous warnings or sanctions	X	x		x	x	x	x