

# Thatto Heath Community Primary School



## **E-Safety Policy**

**Reviewed February 2018**

## Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to

be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

### Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group made up of:

- School E-Safety Coordinator / Officer
- Headteacher
- Teachers
- Support Staff
- ICT Technical staff
- Governors
- Pupils - School Council/Digital Leaders

Consultation with the whole school community has taken place through the following:

- Staff meetings
- School Council
- Link Governor meeting
- Parents evening
- School website

### Schedule for Development / Monitoring / Review

This e-safety policy was approved by the <i>Governors Sub Committee</i> on:	<i>February 2017</i>
The implementation of this e-safety policy will be monitored by the:	<i>The ICT Team and E-Safety Group</i>
Monitoring will take place at regular intervals:	<i>Termly</i>
The <i>Governors Sub Committee</i> will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	<i>December 2017</i>
The E-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 e-safety or incidents that have taken place. The next anticipated review date will be:	<i>February 2018</i>
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	<i>LA ICT Manager, LA Safeguarding Officer, Police Commissioner's Office</i>

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - pupils (eg Ofsted "Tell-us" survey / CEOP ThinkUknow survey)
  - parents / carers
  - staff

## Scope of the Policy

This policy applies to all members of the school community (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 school.

The Education and Inspections Act 2006 empowers Headteachers, 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 e-safety incidents covered by this policy, which may take place out of 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 e-safety behaviour that take place out of school.

## Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

### Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. Mr Chesworth from the school Governing Body has taken on the role of E-Safety Governor as part of his role as the computing curriculum link governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee

### Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator Miss Hamlin.

- The Headteacher and the Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents - included in a later section - "Responding to incidents of misuse" and relevant *Local Authority HR / other relevant body disciplinary procedures*)
- The Headteacher / Co-ordinator is responsible for ensuring that staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.)
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator / Headteacher.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents - included in a later section - "Responding to incidents of misuse" and relevant *Local Authority HR / disciplinary procedures*)

### E-Safety Coordinator - Julia Hamlin

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team
- Holds pupil meetings - Digital Leaders to discuss E Safety matters

### Network Manager / Technical staff:

The Network Manager and ICT Technician are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed

- the school's filtering policy, as directed by the Local Authority is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies
- Respond to E Safety concern forms in relation to network filtering.

### Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction
- digital communications with pupils Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

### Designated person for child protection / Child Protection Officer -Catherine Ireland

Is trained in e-safety issues and be aware of the potential for serious child protection 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

## E-Safety Committee

Members of the E-safety Working Group will assist the E-Safety Coordinator with:

- the production / review / monitoring of the school e-safety policy / documents.
- the production / review / monitoring of the school filtering policy (the school has the St Helens council filtering system).
- Monitoring network / internet / incident logs

## Pupils:

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. At KS1 it would be expected that parents / carers would sign on behalf of the pupils)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

## Parents / 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy and Home/School Agreement.
- accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

## Community Users

Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

## Policy Statements

### Education - students / 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 e-safety is therefore

an essential part of the school's e-safety provision. Children need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT and PHSE and will be regularly revisited - this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages will be reinforced as part of a planned programme of assemblies
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils will be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff will act as good role models in their use of ICT, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that students / 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 are vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

## Education - parents / carers

Many parents and carers have only a limited understanding of e-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 on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

- *High profile events / campaigns eg Safer Internet Day*
- Letters, informational leaflets, newsletters, web site, VL
- Parents evenings
- Reference to the SWGfL Safe website (nb the SWGfL "Golden Rules" for parents)

## Education - Extended Schools

The school will offer family learning courses in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

## Education & Training - Staff

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

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the staff appraisal process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Coordinator/ ICT team will receive regular updates through attendance at training sessions and by reviewing guidance documents released by BECTA / SWGfL / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator / ICT Team will provide advice / guidance / training as required to individuals as required

## Training - Governors

Governors should take part in e-safety training / awareness sessions. 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.

## 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. We also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the E-Safety Committee.

- All users will be provided with a username and password by the ICT Team, who will keep an up to date record of users and their usernames.
- Staff users will be required to change their password every term.
- The "administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher and kept in the school safe.
- Users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by St Helens Council.
- In the event of the Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- Any filtering issues should be reported immediately to St Helens Council.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are available for use by staff to control workstations and view users activity
- An online and paper copy system is in place for users to report any actual / potential e-safety incident to the Network Manager.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Any USB memory sticks must be approved by the ICT team before they can be used in any of the school computers. Staff are issued with encrypted memory sticks.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.
- only the ICT team have permission for the downloading of executable files.
- An agreed policy is in place regarding the extent of personal use that staff and are allowed on laptops and other portable devices that may be used out of school. (see School Personal Data Policy)
- Staff do not have permission for installing programmes on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

### **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 e-safety 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. (see appendix for a more detailed BYOD Policy Template)

- 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 / academy'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

## Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- 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, eg using search engines, staff should be vigilant in monitoring the content of the websites the children visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager 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.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line 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.

## Use of digital and video images - Photographic, Video

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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 eg on social networking sites.
- Staff 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 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 on the website or blog in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. This is done as the pupil start schools

## 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.

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the Headteacher - in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- 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 public chat / social networking programmes must not be used for these communications.
- Whole class or group email addresses will be used at KS1, while pupils at KS2 will be provided with individual school email addresses for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

<i>Communication Technologies</i>	<i>Staff within the school setting</i>				<i>Pupils</i>			
	<i>Allowed</i>	<i>Allowed at certain times</i>	<i>Allowed for selected staff</i>	<i>Not allowed</i>	<i>Allowed</i>	<i>Allowed at certain times</i>	<i>Allowed with staff permission</i>	<i>Not allowed</i>
<i>Mobile phones may be brought to school.</i>	X						<i>Walking Home Y5/6 X</i>	
<i>Use of mobile phones in lessons</i>		X						X
<i>Use of mobile phones in social time</i>	X							X
<i>Taking photos on mobile phones</i>				X				X
<i>Taking photos on school cameras</i>		X					X	
<i>Use of other mobile devices eg tablets, gaming devices</i>		X					X	
<i>Use of personal email addresses in school, or on school network</i>		X						X
<i>Use of school email for personal emails</i>		X						X
<i>Use of messaging apps</i>		X						X
<i>Use of personal social media</i>				X				X
<i>Use of school social media</i>	X						X	
<i>Use of personal blogs</i>				X				X
<i>Use of school blogs</i>	X						X	

Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.

- *Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above will be provided with individual school / academy email addresses for educational use*
- *Students / pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies*
- Personal information should not be posted on the school / academy website and only official email addresses should be 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 e-safety 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, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies 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 / academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise 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. SWGfL BOOST includes unlimited webinar training on this subject: (<http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Professional-Development>)
- 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 students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school /academy or local authority
- Security settings on personal social media profiles are regularly 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 senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

## **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		

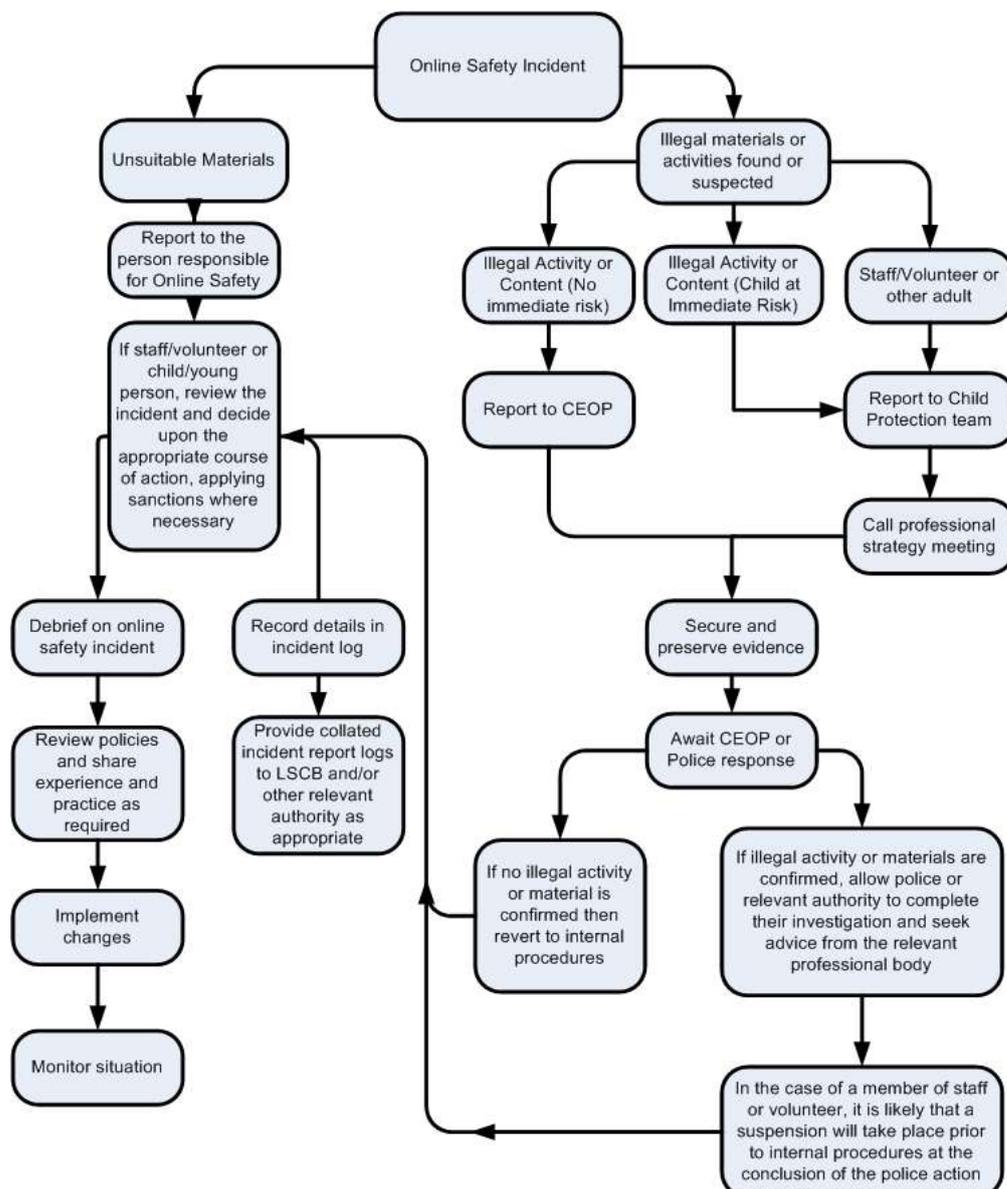
## Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.



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. All such incidents should be report immediately to the Headteacher/ E-Safety Coordinator.

Date on which policy was Reviewed: February 2018

Policy review date: February 2019

Governing Body Committee .....

Date .....

Signed Governor : .....