St Michael with St Thomas C of E Primary School

E-safety Policy

The Three Saints Academy

Date approved: Autumn 2019
Review Date: Autumn 2020

Scope of the Policy

This policy applies to all members of The Three Saints Academy (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the Three Saints Academy's ICT systems, both in and out of the Three Saints Academy. 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 Three Saints Academy's 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 outside of the Three Saints Academy, but is linked to membership of the Three Saints Academy. 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 School's Behaviour Policy.

The Three Saints Academy will deal with such incidents within this policy and associated Safeguarding, 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 e-safety roles and responsibilities of schools, individuals and groups within The Three Saints Academy Trust.

Board of Directors:

Directors 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 Directors receiving regular information.

The Governing Body:

The Governing body of each school will receive regular information, E-Safety incidents and monitoring reports. The Governor responsible for Safeguarding will assume E-Safety responsibilities.

Executive Principal, Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, this is delegated to the Designated Safeguarding

Person (DSP) in respect of e-safety this is in liaison with the ICT Co-ordinator and IT Technician.

- The Headteacher and 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 “Responding to incidents of misuse”.
- The Headteacher is responsible for ensuring that staff are sufficiently trained to carry out their e-safety roles.
- 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 and Governing Body will receive regular monitoring reports from the Designated Safeguarding Person.

Designated Safeguarding Person (DSP):

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents with the ICT Coordinator and IT Technician
- 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 the ICT Co-ordinator and IT Technician (Agilisys)
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, this includes incident logs from staff and from Whisper, an anonymous reporting app on our school website. (See Appendix 5)
- SLT meet to discuss current issues and review incident logs.
- reports regularly to the Governing Body.
- Chairs E-safety group held annually with IT Coordinator and IT Technician.
- 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
  - ✓ risk of radicalisation

ICT Co-ordinator/Agilisys:

Agilisys and the ICT Co-ordinator are responsible for ensuring:

- that the Academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the Three Saints Academy Trust meets required e-safety technical requirements.
- that users may only access the networks and devices through passwords.
- Filtering is applied and updated on a regular basis to ensure:
    - No access to inappropriate internet content, malicious code and other threats;
    - provide controlled social media access;
    - Assist the Academy in meeting the Prevent Duty by keeping children safe from Terrorist and Extremist material
    - Detect expressions that are indicative of cyber bullying or self-destructive patterns.
- that they keep 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/internet/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher for investigation
- that monitoring software/systems are implemented and updated on a regular basis. School currently use Webscreen by Atomwide for filtering and Impero for monitoring within the classroom.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current Three Saints Academy's E-Safety Policy and practices
- they have read, understood and signed the Acceptable User Policy (AUP) annually
- they report any suspected misuse or problem to the Headteacher/Designated Safeguarding Person
- all digital communications with students/pupils/parents/carers 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 activities
- pupils understand and follow the E-safety Policy and AUP and have their own child-friendly version.
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned 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.

Pupils:

- are responsible for using the Three Saints Academy's digital technology systems in accordance with the AUP
- 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 the school's rules on the use of mobile devices and digital cameras. They should also know and understand rules on the taking/use of images and on cyber-bullying (see Anti-bullying policy 2016-19 and child friendly version).
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that The Three Saints Academy'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. The Three Saints Academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, workshops and information about national/local e-safety campaigns/literature. Parents and carers will be encouraged to support the Three Saints Academy in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website
- their children's personal devices in the Three Saints Academy (where this is allowed)

Visitors and Volunteers

Visitors and Volunteers who access the Three Saints Academy's systems/website as part of the wider Three Saints Academy's provision will be expected to sign an AUP before being provided with access to the Three Saints Academy's systems.

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of The Three Saints Academy's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

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

- A planned e-safety curriculum should be provided as part of ICT/PHSE/RSE/other lessons and should be regularly revisited.
- Key e-safety messages should be reinforced as part of the whole school curriculum.
- 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.
- 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.
- Pupils should be supported in building resilience to grooming by providing a safe environment educating pupils to take a responsible approach to recognise and avoid e-safety risks in particular of giving personal information and posting images online.
- Pupils should be helped to understand the need for the AUP and encouraged to adopt safe and responsible use both within and outside the Three Saints Academy Trust.
- 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. This is monitored by the use of Impero and access filtered using Webscreen by Atomwide.
- 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 Agilisys remove those sites from the filtered list for the period of study. Any request to do so, should be approved by the Headteacher.

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 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 Three Saints Academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents/Carers evenings/workshops
- High profile events such as Safer Internet Day
- Links to relevant web sites/publications via the school's website

Education & Training – Staff/Volunteers

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:

- Formal e-safety training is available to staff. This will be regularly updated and enforced.
- Designated Safeguarding Person holds a record of all staff safeguarding training including e-safety training.

All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the Three Saints Academy's E-safety Policy and AUP.

- This E-safety Policy and its updates will be presented to and discussed by staff in termly Department Meetings

- The Designated Safeguarding Person, ICT Coordinator and IT Technician (Agilisys) will provide training to individuals as required.

Training – Governors/Directors

Governors/Directors should take part in e-safety training/awareness sessions either by accessing Governor Training, school training or online training courses that are available.

Technical – infrastructure/equipment, filtering and monitoring

The Three Saints Academy's has a managed ICT service provided by Agilisys.

The Three Saints Academy's technical systems are managed in ways that ensure that the Three Saints Academy's meets recommended technical requirements

- There will be regular reviews and audits of the safety and security of the Three Saints Academy's technical systems
- All users will have clearly defined access rights to the Three Saints Academy's technical systems and devices.
- All staff users are provided with a username and secure password. Users are responsible for the security of their username and password.
- All Pupils up to and including Year 5 log on to computers using a 'class' log on.
- The 'administrator' passwords for each school within the Three Saints Academy's ICT system, used by Agilisys is available to the Headteacher and kept in a secure place (in the school office safe in an envelope).
- Agilisys and the school's ICT Coordinator 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.
- Internet access is filtered for all users**.** Illegal content (child sexual abuse images) is filtered by Agilisys using Webscreen by Atomwide Web Filtering software. 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 (Headteacher's approval required)
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The Three Saints Academy has provided enhanced/differentiated user-level (i.e. pupils do not have access to streaming media whereas staff do).
- Agilisys regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the AUP.
- The system in place for users to report any actual/potential technical incident/security breach is to contact the ICT Co-ordinator or Agilisys.

- 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 Sophos anti-virus software.
- The AUP is in place for the provision of temporary access of “visitors” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- The AUP is in place regarding the personal use that users are allowed on school devices that may be used out of school.

Mobile Technologies (including Bring Your Own Device)

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. Existing mobile technologies such as gaming devices, mobile and smart phones are very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus can open up risk and misuse associated with communication and internet use. All emerging technologies that the school intends to use will be thoroughly examined and tested before implementation in the classroom. We choose to manage the use of the devices in the following ways so that users exploit them appropriately.

All school owned mobile devices are filtered in the same way as all school computing devices via Webscreen by Atomwide. Pupils are restricted from taking the mobile devices from school.

- The school allows staff to bring in personal mobile phones and devices for their own use, they must be switched off during lesson time unless required during an emergency and agreed by the Headteacher. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

- Pupils are allowed to bring mobile phones to school but they must be handed in to the school office upon arrival. If a pupil is found using them for personal reasons during lessons they will be confiscated.

- The sending of inappropriate text, image and video messages between any member of the school community is not allowed.

- Under no circumstance must content created on the mobile device be uploaded to any web site that shares information i.e. Facebook, Instagram, Twitter or YouTube that contains any member of the school community.

- All visitors mobile phones must be switched off while on school site as detailed in the Visitor safeguarding leaflet.

- The Headteacher has the right to take and examine user(s)' devices in the case of misuse as detailed in the school Behaviour Policy.
- Personal mobile phones are not to be used to take and store photographs of pupils even if for school use.

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. 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.

All parents and guardians are asked for permission to use their child's work/photos in the following ways:

- On the schools website
- In the school prospectus and other printed publications that the school may produce for promotional purposes
- Recorded/transmitted on a DVD, video or webcam
- Broadcast on the schools internal multimedia displays
- In display material that may be used in external areas i.e. art exhibitions etc
- General media appearances i.e. local, national media or press releases sent to the press highlighting an activity

This consent form is considered a valid document for the entire duration of the pupil's education at The Three Saints Academy. Pupil names, email, postal address and mobile numbers will not be published against any image.

Storage of Images

- Images of children and staff are stored securely on the school's network.
- Pupils and staff are not permitted to use personal portable media for storage of images.
- Access to these images are only for the school's staff and pupils for school purposes only and use on the school's website.
- The ICT Coordinator is responsible for the deletion of images no longer in use by the school or if the member of staff or pupil has left the school.

CCTV/Webcams

- The school has a CCTV infrastructure for the safety and security of all persons on the site. The only people that have access to CCTV real-time viewing are the Office Admin Staff and SLT.
- Any CCTV footage that is captured for security purposes is only available for viewing by the CEO, Headteacher or their nominated Deputy and the Police.

The school will inform and educate users about these risks:

- When using digital images, staff should inform pupils about the risks associated.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press
- parents/carers are not permitted to take videos and digital images of children at school events.
- Staff are allowed to take digital/video images to support educational aims, but must follow this policy concerning the sharing, distribution and publication of those images. Those images should only be taken on the Three Saints Academy's 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 Three Saints Academy Trust into disrepute.
- pupils must not take, use, share, publish or distribute images of others without their permission
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 (GDPR) 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.

The Three Saints Academy Trust ensures that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”. (Appendix 8)
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed/identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data transfer/storage meets the requirements laid down by the Information Commissioner’s Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected systems.

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

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

- the data must be securely deleted from the device, once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the Three Saints Academy's considers the following as good practice:

- The official Three Saints Academy's email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- A Whisper button is available on the website for staff and pupils to use to report any concerns
- Any digital communication between staff, pupils or parents/carers must be professional in tone and content**.** These communications may only take place on official (monitored) the Three Saints Academy's systems. Personal email addresses, text messaging or social media must not be used for these communications.
- 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 Three Saints Academy's website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Refer to the Three Saints Academy's Acceptable Use Agreement and Social Media Policy.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. The Three Saints Academy Trust 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 Three Saints Academy liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

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

The Three Saints Academy's staff should ensure that:

- No reference should be made in social media to students/pupils, parents/carers or the Three Saints Academy's 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 or Academy.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When the Three Saints Academy's social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under the Three Saints Academy's disciplinary procedures

Personal Use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the Three Saints Academy's or impacts on the school/ academy, it must be made clear that the member of staff is not communicating on behalf of the Three Saints Academy's with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The Three Saints Academy's permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The Three Saints Academy's use of social media for professional purposes will be checked regularly by the ICT Coordinator and IT Technician to ensure compliance with the school policies.

Unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from the Three Saints Academy's 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 Three Saints Academy's believes that the activities referred to in the following section would be inappropriate in the Three Saints Academy's context and that users, as defined below, should not engage in these activities in/or outside the Three Saints Academy's when using the Three Saints Academy's equipment or systems. The Three Saints Academy's 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	
	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 Three Saints Academy's					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	

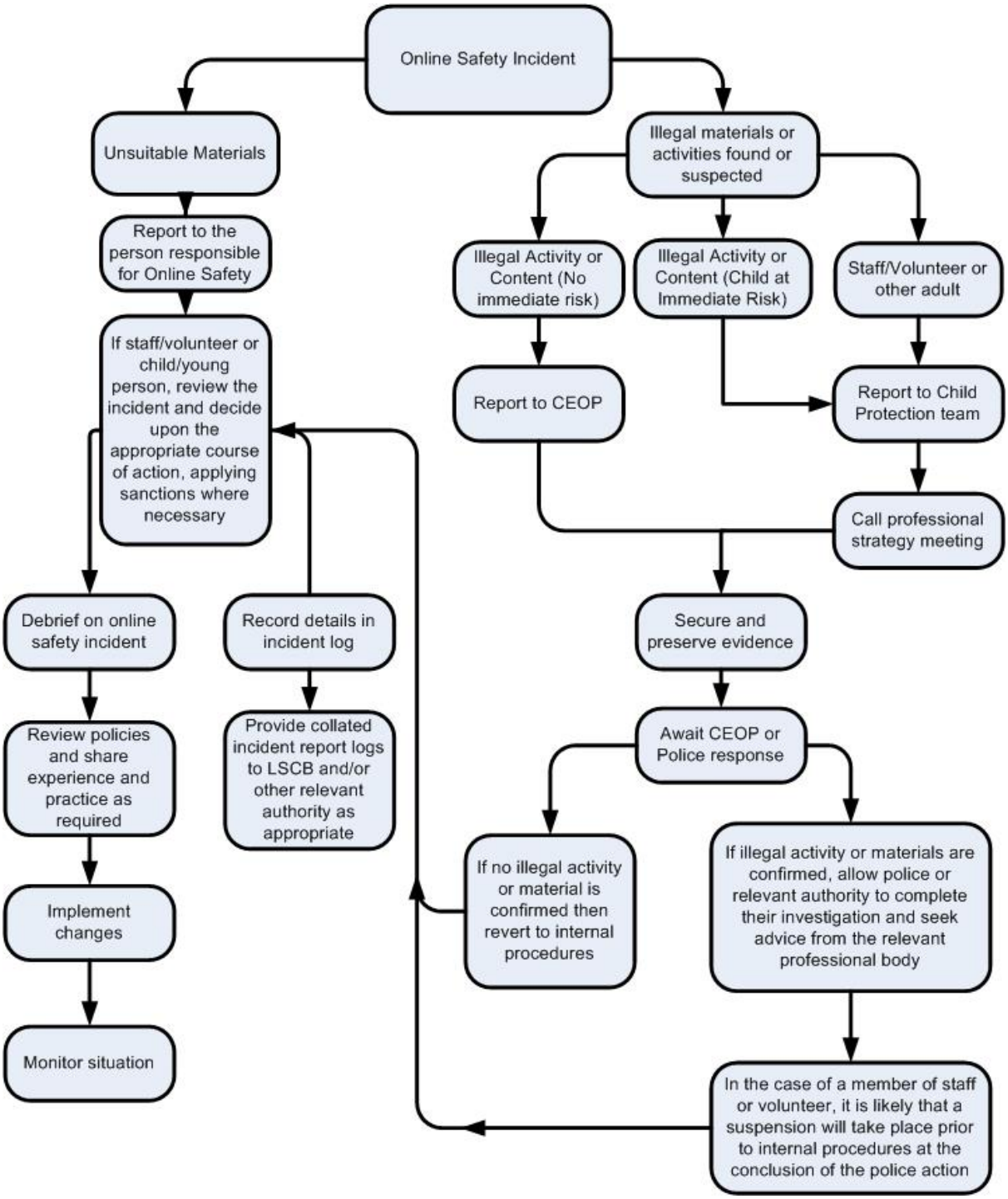
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce				X	
File sharing		X			
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube			X		

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above). Impero reports are generated and monitored by the Headteacher and Agilisys technician.

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 e-safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the Three Saints Academy will be responsible users of digital technologies, who understand and follow the Three Saints Academy's 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 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 SLT 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/Academy Directors 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
    - ✓ promotion of terrorism or extremism
    - ✓ 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 Three Saints 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 DSP for evidence and reference purposes.

The Three Saints Academy's Actions & Sanctions

It is more likely that the Three Saints Academy's will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Pupils Incidents	Refer to class teacher	Refer to Key Stage Leader	Refer to Headteacher/Executive Principal	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Further sanction/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X		X
Unauthorised use of non-educational sites during lessons	X	X	X			X
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X	X			
Unauthorised/inappropriate use of social media/messaging apps/personal email	X	X	X			X
Unauthorised downloading or uploading of files	X	X	X			X
Allowing others to access the Three Saints Academy's network by sharing username and passwords			X			X
Attempting to access or accessing the Three Saints			X			X

Academy's network, using another pupil's account						
Attempting to access or accessing the Three Saints Academy's network, using the account of a member of staff			X			X
Corrupting or destroying the data of other users	X					X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X			X
Continued infringements of the above, following previous warnings or sanctions			X			X
Actions which could bring the Three Saints Academy's into disrepute or breach the integrity of the ethos of the school			X			X
Using proxy sites or other means to subvert the school's/academy's filtering system			X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident			X		X	X
Deliberately accessing or trying to access offensive or pornographic material			X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act 2018			X			X

	Action/Sanctions				
Staff Incidents	Refer to line manager	Refer to Headteacher /Executive Principal	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	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		
Inappropriate personal use of the internet/social media/personal email		X			X
Unauthorised downloading or uploading of files		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
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
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X		X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils		X			X
Actions which could compromise the staff member's professional standing		X			X
Actions which could bring the Three Saints Academy's into disrepute or breach the integrity of the ethos of the Three Saints Academy		X		X	X
Using proxy sites or other means to subvert the school's/academy's filtering system		X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X		X	X

Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X
Breaching copyright or licensing regulations		X			X
Continued infringements of the above, following previous warnings or sanctions		X			X

Appendices

Appendix 1

Acceptable User Policy

Appendix 2

Pupil Acceptable User Policy

Appendix 3

Parent/Carer Use Agreement Form

Appendix 4

Use of Digital /Video Images

Appendix 5

E-safety School Incident Form

Appendix 6

Responding to Incidents of Misuse – flowchart

Appendix 7

Record of reviewing Devices/internet sites

Appendix 8

Privacy Notice

Appendix 9

Legislation

Appendix 10

Links to other organisations or documents

Appendix 11

Glossary of Terms

Appendix 1

Acceptable User Policy

Author/owner: Principals/Directors

Date adopted: 2016

Reviewed: August 2019

Anticipated review: August 2020

Three Saints Academy Trust

Acceptable User Policy

This Acceptable User Policy applies to all staff, pupils and visitors who have access to computers and devices that have access to the internet. Use of the Internet by the fore mentioned users is permitted and encouraged where such use supports the goals and objectives of The Three Saints Academy Trust. Access to the Internet is a privilege and all users must adhere to the policies concerning Computer, Email and Internet usage in line with the Data Protection Act 2018 (GDPR). Violation of these policies could result in disciplinary and/or legal action. All users are required to acknowledge receipt and confirm that they have understood and agree to abide by the rules hereunder and to ensure pupils also abide by these rules.

Computer, email and internet usage

- All users are expected to use the internet responsibly and productively. Internet access on the school's digital hardware resources and systems is limited to work-related activities or for uses deemed 'reasonable' by the Head and/or Governing Body. Personal use is not permitted.

- Work-related activities include research and educational tasks that may be found via the Internet that would help in a user's role.

- All Internet data that is composed, transmitted and/or received by The Three Saints Academy Trust is considered to belong to the trust and is recognised as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.

- Any equipment, services and technology used to access the Internet on the Trust's domain will be monitored and filtered via the web filtering software.

- Emails sent via the school's approved email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images.

- Use the approved school email system or any other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

- All sites and downloads are monitored and can be blocked by Agilisys if they are deemed to be harmful.

- All Internet usage / and network usage is logged and this information could be made available to my manager upon request.

- Ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.

- The installation of software must be approved by the Principal.

- Confidential data transported from one location to another must be protected by encryption following the school's data security protocols when using any such data at any location.

Unacceptable use includes, but is not limited to:

- Allowing unauthorised individuals to access email / Internet / network / or other school / LA systems,
- Stealing, using, disclosing someone else's password or sharing your own.
- Engaging in any online activity that may compromise my professional responsibilities.
- Downloading any software or resources from the Internet that can compromise the network or those that are not adequately licensed.
- Knowingly introducing malicious software onto the network.
- Hacking into unauthorised websites.
- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via The Three Saints email service.
- Accessing work emails on a personal device (including mobile phone) other than via web-based email systems (web mail).
- Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers.
- Browsing, downloading or sending material that could be considered offensive.
- Sending or posting chain letters, solicitations, or advertisements not related to Academy purposes or activities.
- Passing off personal views as representing those of the organisation.

- Sharing confidential material, confidential information, or proprietary information outside of The Three Saints Academy Trust.

- Connecting a computer, laptop or other device to the network / Internet that does not have up-to-date anti-virus software.

- Connecting a USB (flash drive) to a computer, laptop or other device on the network (reminder: all staff employed by The Three Saints Academy Trust have a personal Microsoft Office One Drive which should be used to store and transport data securely)

- Using personal digital cameras or camera phones for taking and transferring images of pupils or staff.

If a User is unsure about what constitutes Acceptable Internet usage, then he/she should ask his/her ICT Coordinator for further guidance and clarification.

All terms and conditions as stated in this document are applicable to all users of The Three Saints Trust network and Internet connection. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures mentioned above. Any user violating these policies is subject to disciplinary actions deemed appropriate by the Directors.

User compliance

I understand and will abide by this Acceptable Usage Policy. I further understand that should I commit any violation of this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

I agree to have an email account, be connected to the Internet and be able to use the school's ICT resources & systems.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

User Signature

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

Authorised Signature (Head Teacher)

I approve this user to be set-up.

Signature ..... Date .....

Full Name ..... (printed)

Appendix 2

Pupil Acceptable User Policy

(Acceptable ICT User Policy)

Author/owner: Principals/Directors

Date adopted: 2016

Reviewed: September 2019

Anticipated review: August 2020

Pupils will have the Acceptable ICT User Policy explained to them. They will be asked to sign a copy, which will then be displayed within the classroom as a reminder of what they have agreed to. All children will be made aware that the staff can monitor what the children are accessing from their computer screen via monitoring software and can also lockdown their computer and take a screenshot/video recording of what they are accessing.

Foundation and KS1

- I will take care when I use computers, as I know they are very expensive.
- I know I can ask for help if I am stuck.
- I will do what I am asked to do, by the teacher.
- If I don't follow the rules, I will not be able to use the computers

KS2

- I will not access computers without permission.
- I will only use programs & websites that I am instructed to use.
- I will immediately tell an adult if I see something that I don't like.
- I will treat the school equipment as if it was my own.
- I understand that if I don't follow the rules above, I will not be able to use the computers.

Appendix 3

Parent/Carer Permission Form

Parent/Carers Name: ……

Pupil Name: ……..

As the parent/carer of the above *pupil*, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I understand that the school has discussed the Acceptable Use Agreement with my son/daughter and that they have received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed: .....

Date: .....

Appendix 4

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Students/Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree

Digital/Video Images Permission Form

Parent/Carers Name: .....

Pupil Name: .....

As the parent/carer of the above student/pupil, I agree to the school taking and using digital/video images of my child/children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school. Yes/No

Signed: .....

Date: .....

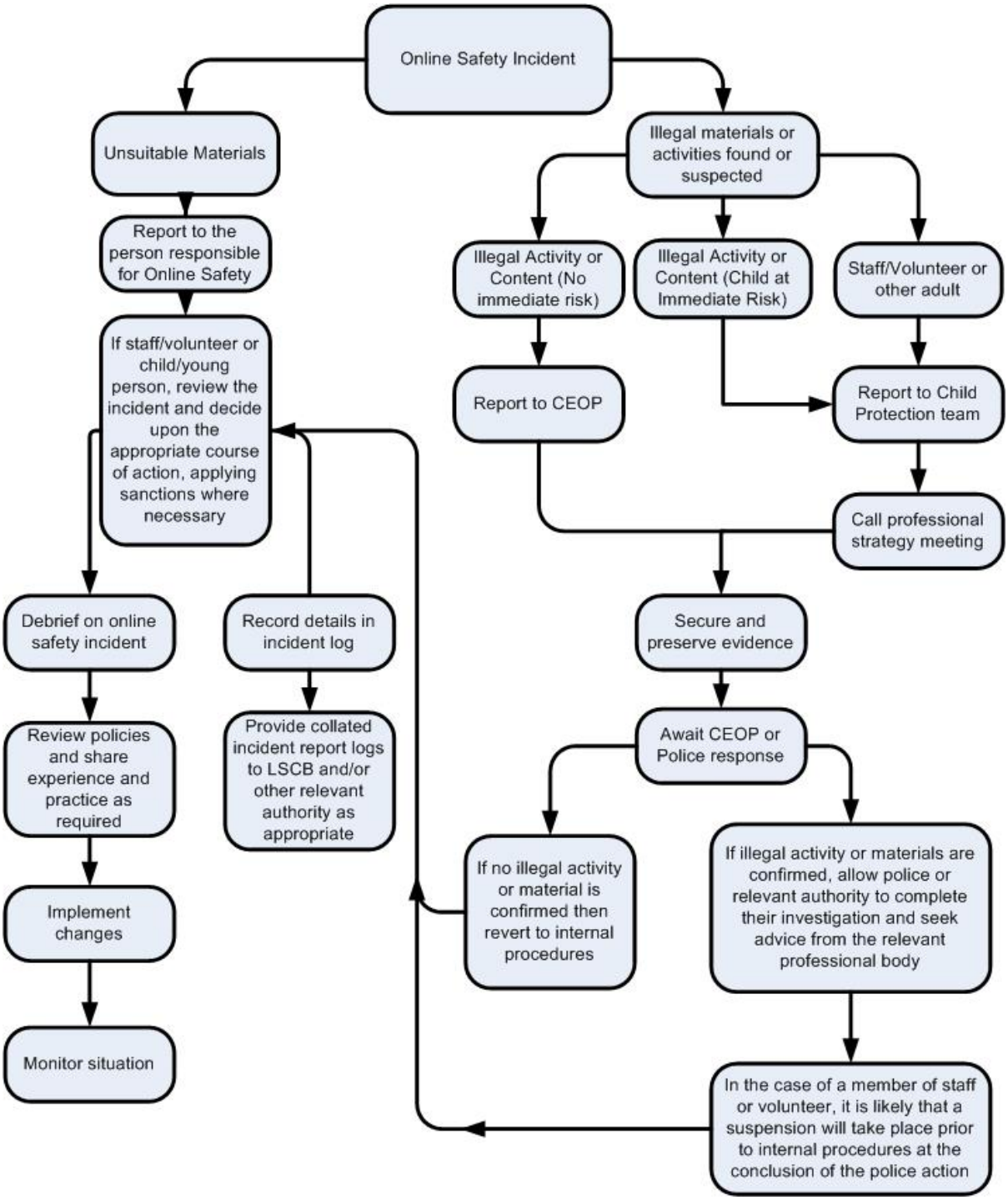
Appendix 5

PUPIL E-SAFETY INCIDENT FORM

Date and time of incident:		
Where did the incident occur? ie At School or at home:		
Who was involved in the incident?		
Child/Young Person ☐	**Name:**	
Staff Member/Volunteer ☐	**Name:**	
Description of incident		
Action Taken	**☐ Incident Reported to Headteacher/Snr Manager** **☐ Advice Sought from Social Care** **☐ Referral made to Social Care** **☐ Incident Reported to the Police** **☐Incident Reported to CEOP** **☐ Disciplinary Action Taken** **☐E-safety Policy to be reviewed/amended** **☐ Other (please specify) …… ……**	
Outcome of investigation:		

Signature of worker:		**Dated:**
Signature of Supervisor/Manager:		**Dated:**

Responding to incidents of misuse – flow chart



Appendix 7

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)

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Appendix 8

PRIVACY NOTICE

We St Michael with St Thomas CE are the Data Controller for the purposes of the Data Protection Act. We collect information from you regarding your child, and may receive information from your child's previous school. We hold this personal data and use it to:

- Support your child's teaching and learning;
- Monitor and report on your child's progress;
- Provide appropriate pastoral care, and
- Assess how well your child is doing.

This information includes your contact details, national curriculum assessment results, attendance information. You will sign a form when you enrol your child at school, which gives your permission for specific activities we carry out, and characteristics such as ethnic group, special educational needs and any relevant medical information.

We will not give permission about your child to anyone outside the school without your consent unless the law and our rules permit it.*

We are required by law to pass some of your information to the Halton Children's Social Care Team, and the Department for Education (DFE).

If you want to see a copy of the information we hold and share about your child then please contact the School Office.

If you require more information about how the school, Halton CSC and/or DCSF store and use this data you can either pick up a full text version of the Privacy Notice from the School Office. Alternatively, if you have internet access you can download these documents from the following websites:

- http://www.teachernet.gov.uk/doc/13856/DCSF%20what%20we%20do%20with%20Children's%20data%20v4%20final.doc
- https://www3.halton.gov.uk/Pages/councildemocracy/pdfs/dataprotection/DataProtectionPolicy.pdf

Appendix 9

Legislation

Schools should be aware of the legislative framework under which this E-safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 2018 (GDPR)

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or

persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with

whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE).

Counter Terrorism and Security Act 2015

Section 29 duty on schools and teachers in respect of statutory Prevent Duty Guidance for schools.

Appendix 10

Links to other organisations or documents

The following links may help those who are developing or reviewing a school e-safetypolicy:

UK Safer Internet Centre

Safer Internet Centre – http://saferinternet.org.uk/
South West Grid for Learning - http://swgfl.org.uk/
Childnet – http://www.childnet-int.org/
Professionals E-safetyHelpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/

Tools for Schools

E-safetyBOOST – https://boost.swgfl.org.uk/
360 Degree Safe – E-safetyself-review tool – https://360safe.org.uk/

Bullying/Cyberbullying

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – new Cyberbullying guidance and toolkit (Launch spring/summer 2016) - http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming-cyberbullying-work
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks

SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people
Connectsafely Parents Guide to Facebook
Facebook Guide for Educators

Curriculum

SWGfL Digital Literacy & Citizenship curriculum
Glow - http://www.educationscotland.gov.uk/usingglowandict/
Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Mobile Devices/BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking
NEN - Guidance Note - BYOD

Data Protection

Information Commissioners Office:

Your rights to your information – Resources for Schools - ICO
Guide to Data Protection Act - Information Commissioners Office
Guide to the Freedom of Information Act - Information Commissioners Office
ICO guidance on the Freedom of Information Model Publication Scheme
ICO Freedom of Information Model Publication Scheme Template for schools (England)
ICO - Guidance we gave to schools - September 2012 (England)
ICO Guidance on Bring Your Own Device
ICO Guidance on Cloud Hosted Services
Information Commissioners Office good practice note on taking photos in schools
ICO Guidance Data Protection Practical Guide to IT Security
ICO – Think Privacy Toolkit
ICO – Personal Information Online – Code of Practice
ICO Subject Access Code of Practice
ICO – Guidance on Data Security Breach Management
SWGfL - Guidance for Schools on Cloud Hosted Services
LGfL - Data Handling Compliance Check List
Somerset - Flowchart on Storage of Personal Data
NEN - Guidance Note - Protecting School Data

Professional Standards/Staff Training

DfE - Safer Working Practice for Adults who Work with Children and Young People
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf
Childnet/TDA - Social Networking - a guide for trainee teachers & NQTs
Childnet/TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
UK Safer Internet Centre Professionals E-safetyHelpline

Infrastructure/Technical Support

Somerset - Questions for Technical Support
NEN - Guidance Note - esecurity

Working with parents and carers

SWGfL Digital Literacy & Citizenship curriculum
E-safetyBOOST Presentations - parent's presentation
Connectsafely Parents Guide to Facebook
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Insafe - A guide for parents - education and the new media
The Cybersmile Foundation (cyberbullying) - advice for parents

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
Futurelab - "Digital participation - its not chalk and talk any more!"
Ofcom – Children & Parents – media use and attitudes report - 2015

Appendix 11

Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational e-safety programmes for schools, young people and parents.

VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.