



## **E-safety Policy**

**Author/owner: Headteacher/ Directors**

**Date adopted: Spring 2016, 2020**

**Anticipated review: Spring 2023**

## **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 Relationships & 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 School Committee:**

The School Committee of each school will receive regular information, E-Safety incidents and monitoring reports.

### **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 Computing Lead 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 School Committee will receive regular monitoring reports from the Designated Safeguarding Person.

## Designated Safeguarding Lead (DSL):

- takes day to day responsibility for e-safety issues/ documents with the Computing Lead 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 Computing Lead and IT Technician (Agilisys)
- receives notification of e-safety incidents to inform future e-safety developments, this includes CPOMS e-safety logs from staff and from Need to Talk Button, a reporting app on our school website.
- SLT meet to discuss current issues and review incidents.
- reports regularly to the School Committee.
- chairs E-safety group held annually with Computing Lead and Agilisys 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

## Computing Lead/Agilisys:

Agilisys and the Computing Lead is 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 Lead
- 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 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 mentoring conversations, 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 agree to the AUP on sign in before being able to access 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 Computing / 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 (eg 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 Lead 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 Lead, Computing Lead and Agilisys will provide training to individuals as required.

## Training – School Committee/ 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 are provided with their own username and password.
- 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 (eg the school office safe)
- Agilisys and the school's Computing Lead 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 will ensure that children are safe from terrorist and extremist material when accessing the internet.
- The Three Saints Academy has provided enhanced / differentiated user-level (ie 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 Computing Lead 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 virus software.
- The AUP is on sign in to The Three Saints Academy school systems 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 removing 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. The school does not permit members of staff to contact a pupil or parent/carer using their personal device, unless they are working remotely. In which case staff must dial 141 prior to making the call so the number is withheld.
- Pupils are allowed to bring mobile phones to school but they must be handed in to their teacher 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, IChat or YouTube that contains any member of the school community.
- All visitor's 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 users' devices in the case of misuse as detailed in the school Relationships and 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 school's 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 school's 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 issued to parents when their child commences 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 and social media sites.
- The Computing Lead in liaison with Agilysis 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.

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 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
- 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 devices.

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

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, 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.
- The School Website has a Need to Talk reporting button for pupils to communicate with school.
- 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 a 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 Computing Lead and Agilysis 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	

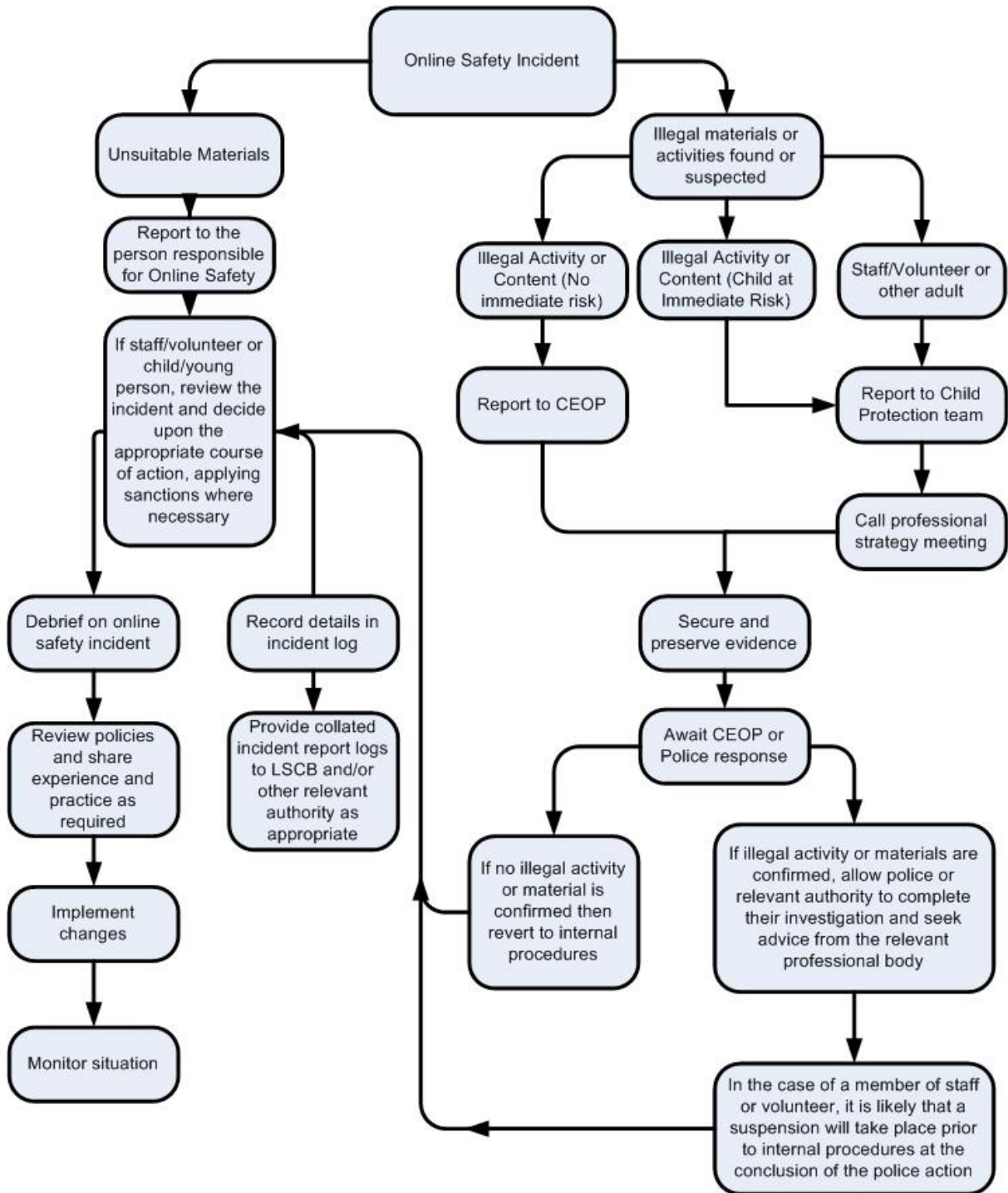
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)			X	
On-line gaming (educational)	X			
On-line gaming (non-educational)			X	
On-line gambling			X	
On-line shopping / commerce			X	
File sharing	X			
Use of social media		X		
Use of messaging apps		X		
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).

# 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 DSL 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			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 Academy's network, using another pupil's account			X			X
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 GDPR			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**

Parent/Carer Use Agreement Form

## **Appendix 2**

Trust Photograph Consent Form

## **Appendix 3**

Responding to Incidents of Misuse – flowchart

## **Appendix 4**

Record of reviewing Devices/internet sites

## **Appendix 5**

Privacy Notice

## **Appendix 6**

Legislation

## **Appendix 7**

Links to other organisations or documents

## **Appendix 8**

Glossary of Terms

# Appendix 1



**Rainhill St Ann's CE Primary School**  
View Road, Rainhill, Merseyside, L35 0LQ  
Tel 0151 426 5869, [www.rainhillstanns.co.uk](http://www.rainhillstanns.co.uk)  
Email: [stannsce@three-saints.org.uk](mailto:stannsce@three-saints.org.uk)  
Twitter: [@StAnnsRainhill](https://twitter.com/StAnnsRainhill)  
Headteacher: Mrs Laura Rvnnl



CHILDS NAME \_\_\_\_\_ CLASS \_\_\_\_\_

## General consent form

This consent form contains several general permission requests that will be completed on an annual basis whilst your child is a pupil at St Ann's, these consents can also be completed on the Parent Portal on Arbor

	Yes	No
I give consent for my child to take part in school trips/ visits that take place in the local area and involve walking from school to the destination and back. These trips/ visits could involve: St Ann's Church, Swimming Baths, Rainhill High School etc but this list is not exhaustive. Individual permission slips will not be sought for this but you will be informed that these events are happening. For trips which involve transporting your child or for residential trips, separate letters will be sent out requesting your permission		
I give consent for my child to be given first aid or urgent medical treatment in school, during any school trip or activity		
I give consent for my child to access the internet and other computer-based programmes whilst in school. I understand that a filtering system is used in school to prevent pupils from accessing objectionable material. Please note that a more comprehensive "Pupil & Parent Acceptable User Policy" form will also be issued annually		
I give consent for my child to have milk at school (EYFS, Year 1 & 2 only for annual payment of £6)		
I give consent for my child to be provided with the school's emergency inhaler should they require it		

## Medical Information

Please provide details of any medical condition that your child suffers from and any medication they should take during off-site visits in the space provided below.

If you object to any element of the above, please state the objection against the relevant permission statements. This consent form lasts the duration of this academic year and will be updated on an annual basis. If you wish to make any changes, please contact the school office.

Signed:

\_\_\_\_\_ Date: \_\_\_\_\_

## Appendix 2

# The Three Saints Academy Trust



## Photographs and Video Consent Form

Photographs and videos will only be collected and stored with a documented lawful basis.

Photographs and videos will be used where they are deemed essential for performing the public task of the school and evidencing the school curriculum/ school events. Where photographs are required for other purposes, these purposes will be documented and explicit consent sought.

The retention period for photographs and videos will be documented in the retention policy. At the end of the retention period photographs will either be destroyed, or may be retained for archiving purposes in the public interest.

Please also note that when your child is in a public venue local media may take photos. You are able to object to this processing and we will give you prior knowledge if and when we know third-parties will be present at external events.

Where local media come into the school to take photographs, we will ask for consent for that specific purpose beforehand.

Where photographs are used as part of a display we will not accompany the photograph with any other identifiable information such as names.

Photographs and video will only be taken using school equipment and must represent the school and children positively – inappropriate, negative, embarrassing or distressful photos will not be used. Consent will be sought from parents/carers.

Where parental consent has been obtained we will use this lawful basis until the data subject can demonstrate their understanding to either confirm or withdraw their own consent.

We collect and use photographs/videos for the following purposes.

Please tick the box to confirm you agree to the use of photographs/videos for that purpose:

	<b>Photographs/Videos</b>
For <b>display in school</b> (including corridors, classrooms and reception area)	
For use in <b>school/trust publications</b> including newsletter and other printed/e mailed documents (such as the prospectus) and their publication on the <b>school/trust website</b>	
For use on <b>social media</b> (such as the school Twitter or Facebook page)	
School photographs/videos can be provided to the <b>media for publication or broadcast</b>	
<b>Programmes for School Performances</b> (the child’s photograph will be accompanied by the child’s first name)	

I have read and understood the information.

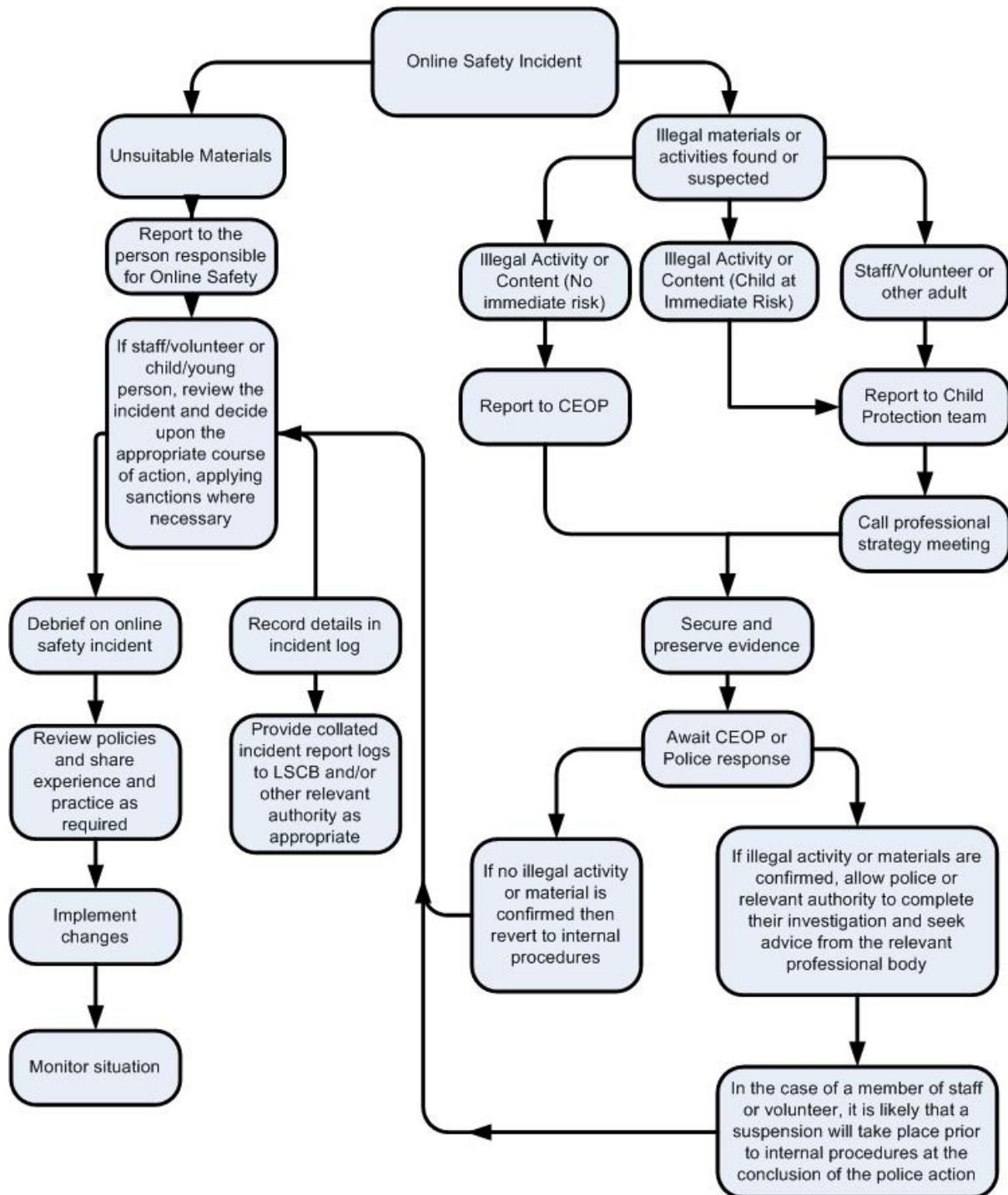
I agree for my / my child’s photographs and video to be used for the purposes described.

Pupil Name	
Name of parent/carer	
Signature of parent/carer	
Date:	

**If you wish to withdraw consent, please ask the school office for a consent withdrawal form**

## Appendix 3

Responding to incidents of misuse – flow chart



**Appendix 4**

# 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 5 – St Ann’s CE Primary School**

### **PRIVACY NOTICE**

Please click on the following link for the Trust Privacy Notice:

<http://www.three-saints.org.uk/files/1716/0274/9216/TrustPrivacyNotice-ParentsPupils.pdf>

## Appendix 6 - Whole document new version uploaded

### Legislation

Schools/academies should be aware of the legislative framework under which this online 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 online 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.

School/academies may wish to view the National Crime Agency website which includes information about [“Cyber crime – preventing young people from getting involved”](#). Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful [summary of the Act on the NCA site](#).

#### Data Protection Act 1998

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.

#### The Data Protection Act 2018 (GDPR):

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.

- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

### 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 Harassment 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 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.

<http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation>

### 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:

<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

### Serious Crime Act 2015

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

### Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the [Revenge Porn Helpline](#)

## Appendix 7 – Fully updated

# Links to other organisations or documents

### UK Safer Internet Centre

Safer Internet Centre – <https://www.saferinternet.org.uk/>

South West Grid for Learning - <https://swgfl.org.uk/products-services/online-safety/>

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Revenge Porn Helpline - <https://revengepornhelpline.org.uk/>

Internet Watch Foundation - <https://www.iwf.org.uk/>

Report Harmful Content - <https://reportharmfulcontent.com/>

### CEOP

CEOP - <http://ceop.police.uk/>

ThinkUKnow - <https://www.thinkuknow.co.uk/>

### Others

[LGfL – Online Safety Resources](#)

[Kent – Online Safety Resources page](#)

INSAFE/Better Internet for Kids - <https://www.betterinternetforkids.eu/>

UK Council for Internet Safety (UKCIS) - <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

Netsmartz - <http://www.netsmartz.org/>

### Tools for Schools

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

360Data – online data protection self-review tool: [www.360data.org.uk](http://www.360data.org.uk)

SWGfL Test filtering - <http://testfiltering.com/>

UKCIS Digital Resilience Framework - <https://www.gov.uk/government/publications/digital-resilience-framework>

### Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

SELMA – Hacking Hate - <https://selma.swgfl.co.uk>

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](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf)

Childnet – Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>

[Childnet – Project deSHAME – Online Sexual Harrassment](#)

[UKSIC – Sexting Resources](#)

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

[Ditch the Label – Online Bullying Charity](#)

[Diana Award – Anti-Bullying Campaign](#)

## Social Networking

Digizen – [Social Networking](#)

UKSIC - [Safety Features on Social Networks](#)

[Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media](#)

## Curriculum

SWGfL Evolve - <https://projectevolve.co.uk>

[UKCCIS – Education for a connected world framework](#)

Teach Today – [www.teachtoday.eu/](http://www.teachtoday.eu/)

Insafe - [Education Resources](#)

## Data Protection

[360data - free questionnaire and data protection self review tool](#)

[ICO Guides for Education \(wide range of sector specific guides\)](#)

[DfE advice on Cloud software services and the Data Protection Act](#)

[IRMS - Records Management Toolkit for Schools](#)

[NHS - Caldicott Principles \(information that must be released\)](#)

[ICO Guidance on taking photos in schools](#)

[Dotkumo - Best practice guide to using photos](#)

## Professional Standards/Staff Training

[DfE – Keeping Children Safe in Education](#)

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)

[Childnet – School Pack for Online Safety Awareness](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

## Infrastructure/Technical Support

[UKSIC – Appropriate Filtering and Monitoring](#)

[SWGfL Safety & Security Resources](#)

Somerset - [Questions for Technical Support](#)

NCA – [Guide to the Computer Misuse Act](#)

NEN – [Advice and Guidance Notes](#)

## Working with parents and carers

[Online Safety BOOST Presentations - parent's presentation](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops/education](#)

[Internet Matters](#)

## Prevent

[Prevent Duty Guidance](#)

[Prevent for schools – teaching resources](#)

[NCA – Cyber Prevent](#)

Childnet – [Trust Me](#)

## Research

[Ofcom –Media Literacy Research](#)

Further links can be found at the end of the UKCIS [Education for a Connected World Framework](#)

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

## Appendix 8 – fully updated

# Glossary of Terms

<b>AUP/AUA</b>	Acceptable Use Policy/Agreement – see templates earlier in this document
<b>CEOP</b>	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
<b>CPD</b>	Continuous Professional Development
<b>FOSI</b>	Family Online Safety Institute
<b>ICO</b>	Information Commissioners Office
<b>ICT</b>	Information and Communications Technology
<b>INSET</b>	In Service Education and Training
<b>IP address</b>	The label that identifies each computer to other computers using the IP (internet protocol)
<b>ISP</b>	Internet Service Provider
<b>ISPA</b>	Internet Service Providers’ Association
<b>IWF</b>	Internet Watch Foundation
<b>LA</b>	Local Authority
<b>LAN</b>	Local Area Network
<b>MAT</b>	Multi Academy Trust
<b>MIS</b>	Management Information System
<b>NEN</b>	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
<b>Ofcom</b>	Office of Communications (Independent communications sector regulator)
<b>SWGfL</b>	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
<b>TUK</b>	Think U Know – educational online safety programmes for schools, young people and parents.
<b>UKSIC</b>	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
<b>UKCIS</b>	UK Council for Internet Safety
<b>VLE</b>	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
<b>WAP</b>	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS [Education for a Connected World Framework](#)

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty

arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.