Online Safety Policy

Author/owner: Principals/Directors

Date adopted: Spring 2016, 2020, 2023

Anticipated review: Spring 2026

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. It also applies to the use of personal digital technology on the school site (where allowed). 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 online-bullying or online 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 and Relationships 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 online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online 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 Online 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, online safety incidents and monitoring reports. The School Committee Safeguarding Member is responsible for ensuring that the filtering and monitoring provision is reviewed.

Headteacher (DSL) and Senior Leaders:

- The Headteacher (DSL) has a duty of care for ensuring the safety (including online safety) of members of the school community this is in liaison with the IT Lead and IT Technician.
- The Headteacher (DSL) takes day to day responsibility for online safety issues.
- The Headteacher (DSL) and Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents "Responding to incidents of misuse".
- The Headteacher (DSL) is responsible for ensuring that technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant
- The Headteacher (DSL) ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- The Headteacher (DSL) is responsible for ensuring that staff are sufficiently trained to carry out their online safety roles.
- The Headteacher (DSL) will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team and School Committee will receive regular monitoring reports from the Headteacher (DSL).
- The Headteacher (DSL) liaises with the Local Authority
- The Headteacher (DSL) liaises with the IC Lead and IT Technician (Agilisys)
- The Headteacher (DSL) receives notification of online safety incidents to inform future online safety developments, this includes CPOMS online safety logs from staff and from the Need to Talk Button, a reporting app on the school website.
- SLT meet to discuss current issues and review incidents.
- The Headteacher (DSL) reports regularly to the School Committee.
- The Headteacher (DSL) chairs the online safety group held annually with IT Lead and Agilisys IT Technician.
- The Headteacher (DSL) is trained in online safety issues and is 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
  - ✓ online bullying
  - ✓ risk of radicalisation

IT Lead/Agilisys:

Agilisys and the ICT 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 online safety technical requirements.
- that users may only access the networks and devices through passwords.
- Filtering and monitoring 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 online bullying or self-destructive patterns.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher (DSL) for investigation. *The Trust's IT provider Agilisys monitors and controls the firewall and internet filtering system by utilising the ADEPT Education filtering system on the LGFL network.*
- that monitoring and filtering software / systems are implemented and updated on a regular basis. School currently use School Protect: Webscreen for filtering and Impero for monitoring within the classroom. *School Protect: Webscreen filtering checks are completed by the IT technician monthly using the SWGfL testing tool and reported to the Headteacher (DSL).*
- *Spot checks of staff having IMPERO open is undertaken by the IT technician and reported to the Headtecher at least half termly with action taken were necessary.*
- Impero alerts are monitored daily. Alert MONITORING reports are scheduled weekly.

Curriculum Leads

Curriculum Leads will work with the Headteacher (DSL) to develop a planned and coordinated online safety education programme in conjunction with

Dfe Guidance Teaching Online Safety in Schools.

This will be provided through:

- PHSE and RSE programmes
- A mapped cross-curricular programme

- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current Three Saints Academy's Online safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood and signed the Acceptable User Policy (AUP) annually
- they report any suspected misuse or problem to the Headteacher (DSL) / 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
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online 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 supervise and 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.
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

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
- should know what to do if they or someone they know feels vulnerable when using online technology
- 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 online-bullying (see Anti-bullying policy and child friendly version).
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that The Three Saints Academy's Online 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 online safety campaigns / literature.

Parents and carers will be encouraged to support the Three Saints Academy in promoting good online 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.

Online Safety Group

The Online Safety Group is a consultative group with responsibility for issues regarding online safety:

- the review/monitoring of the school monitoring and filtering standards and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs
- encouraging the contribution of pupils to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- completion and monitoring improvement actions identified through use of the 360-degree safe self-review tool.

The Online Safety Group has the following members:

- Headteacher (DSL/Online Safety Lead)
- Technical staff
- Curriculum lead
- Pupil voice will be sought to feed into the group.

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Policy

The Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard pupils in the digital world
- describes how the school will help prepare pupils to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and via the shared policy teams folder

- is published on the school website.

Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- staff induction and code of conduct
- splash screens
- AUP signage
- communication with parents/carers
- built into education sessions

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKCIS Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks,					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Act (1990)	data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent pupils becoming involved in cyber-crime and harness their activity in positive ways – further information here					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school (with authorization mobile hotspots may be allowed)				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes: Schools may wish to add further activities to this list.	Staff and other adults				Pupils			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming			X				X	
Online shopping/commerce	X				X			
File sharing			X				X	
Social media				X	X			
Messaging/chat				X	X			
Entertainment streaming e.g. Netflix, Disney+	X				X			
Use of video broadcasting, e.g. YouTube			X		X			
Mobile phones may be brought to school		X						X
Use of mobile phones for learning at school	X				X			
Use of mobile phones in social time at school		X			X			
Taking photos on mobile phones/cameras	X				X			
Use of other personal devices, e.g. tablets, gaming devices				X	X			

Use of personal e-mail in school, or on school network/wi-fi	X				X			
Use of school e-mail for personal e-mails	X				X			

When using communication technologies, the Trust considers the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school
- any digital communication between staff and pupils or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. **Personal e-mail addresses, text messaging or social media must not be used for these communications.**
- staff are expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to the Headteacher (DSL) – in accordance with the school policy – 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

  Relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and pupils.

Reporting and responding

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of pupils. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

> *"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:*
>
> - *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"*

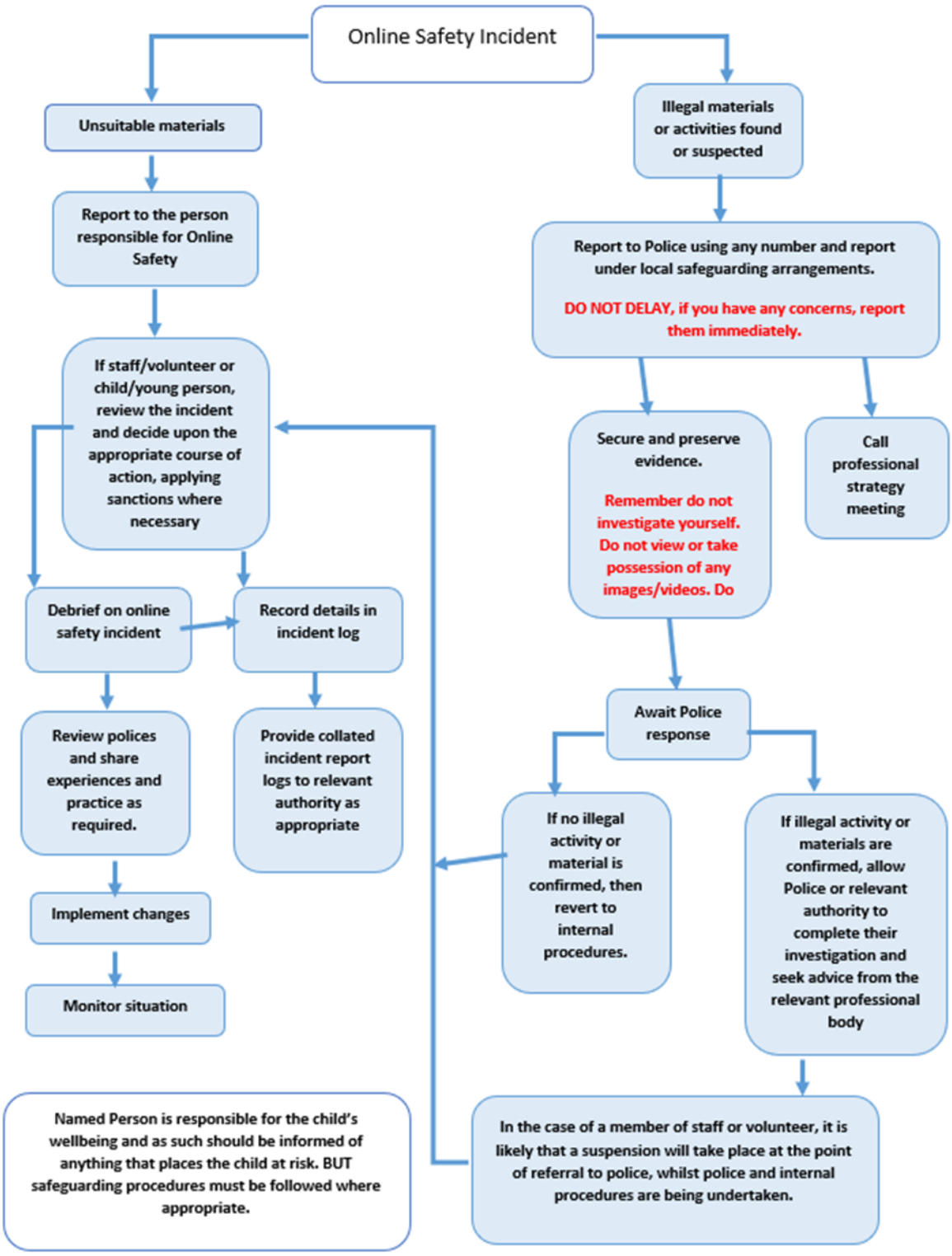
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents

- reports will be dealt with as soon as is practically possible once they are received
- the Headteacher (DSL), and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures.
- any concern about staff misuse will be reported to the Headteacher (DSL), unless the concern involves the Headteacher (DSL), in which case the complaint is referred to the Chair of the School Committee and the MAT CEO
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by pupils and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff 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
    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by local authority / MAT (as relevant)
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged via CPOMS in respect of pupils.
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions as appropriate
- learning from the incident (or pattern of incidents) will be provided to:
    - the Online Safety Group for consideration of updates to policies or curriculum and to review how effectively the report was dealt with

- staff, through regular briefings
- pupils, through assemblies/lessons
- parents/carers, through newsletters, school social media, website
- school committee members, through regular safeguarding updates
- local authority/external agencies, as relevant

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

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:

Responding to Pupil Actions

Incidents	Refer to class teacher/tutor	Refer to Head of Department / Principal Teacher / Deputy Head	Refer to Headteacher (DSL)	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		**X**	**X**	**X**			x		
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords	X	X	X			X		X	X
Corrupting or destroying the data of other users.	X	X	X			X	X	X	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X		X	X
Unauthorised downloading or uploading of files or use of file sharing.	X	X	X			X	X	X	X
Using proxy sites or other means to subvert the school's filtering system.			X				X	X	X

Incidents	Refer to class teacher/tutor	Refer to Head of Department / Principal Teacher / Deputy Head	Refer to Headteacher (DSL)	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Accidentally accessing offensive or pornographic material and failing to report the incident.	X								
Deliberately accessing or trying to access offensive or pornographic material.		X	X			X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X		X					X	
Unauthorised use of digital devices (including taking images)			X			X		X	
Unauthorised use of online services	X						X		
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.			X						
Continued infringements of the above, following previous warnings or sanctions.							X		X

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher (DSL)/ Principal	Refer to local authority/MAT/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X				
Deliberate actions to breach data protection or network security rules.		X			X	X		
Deliberately accessing or trying to access offensive or pornographic material		X			X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X		X			
Using proxy sites or other means to subvert the school's filtering system.	X							
Unauthorised downloading or uploading of files or file sharing	X							
Breaching copyright or licensing regulations.	X					X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.		X	X		X			X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X						
Using personal e-mail/social networking/messaging to carry out digital communications with pupils and parents/carers		X	X			X		X

Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X					X		
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner			X					X
Actions which could compromise the staff member's professional standing		X						
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X	X			X		
Failing to report incidents whether caused by deliberate or accidental actions	X	X						
Continued infringements of the above, following previous warnings or sanctions.			X		X		X	X

Policy Statements

Education – Pupils

While regulation and technical solutions are particularly important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of The Three Saints Academy's online safety provision. Pupils need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:

> *"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'.."*

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

- A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes

- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to pupils at different ages and abilities such as those with additional learning needs or those with English as an additional language**.**
- pupils should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where pupils are allowed to freely search the internet, staff should be vigilant in supervising the pupils and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Pupil Contribution

The Three Saints Academy acknowledges, learns from, and uses the skills and knowledge of pupils in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for each school's community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- *mechanisms to canvass pupil feedback and opinion.*
- *appointment of digital leaders/anti-bullying ambassadors/well-being ambassadors*
- *the Online Safety Group has contributions from pupils*
- *pupils contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns*
- *pupils designing/updating acceptable use agreements*
- *contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.*

Staff/volunteers

The DfE guidance "Keeping Children Safe in Education" states:

> "All staff should receive appropriate safeguarding and child protection training (including online safety) at induction. The training should be regularly updated. In addition, all staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."
>
> "Governing bodies and proprietors should ensure... that safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning.**"**

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- the Online Safety Lead/ Designated Safeguarding Lead will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MAT / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the Online Safety Lead/DSL will provide advice/guidance/training to individuals as required.

School Committee/Directors

School Committee members and Directors take part in online safety training/awareness sessions, This may be offered in several ways such as:

- attendance at training provided by the MAT or other relevant organisation including online training
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

Families

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

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

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
- the pupils – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by pupils leading sessions at parent/carer evenings.
- letters, newsletters, website, learning platform,
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).
- Sharing good practice with other schools in clusters and or the local authority/MAT.

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

Filtering

- the Trust manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering.
- access to online content and services is managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content
- there is a clear process in place to deal with requests for filtering changes

- *the school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)*
- filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
- *where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.*
- *access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.*

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

See Filtering and Monitoring Standards Appendix 1.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- There is a staff lead responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school's risk assessment. These include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- *pro-active alerts inform the school of breaches, allowing effective intervention.*
- *where possible, school technical staff regularly monitor the activity of users on the school technical systems*

- 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. Year 6 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 (DSL) and kept in a secure place (eg the school office safe)
- Agilisys and the school's ICT 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 School Protect: Webscreen 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 (DSL)'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 IT 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 system 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.

See Filtering and Monitoring Standards Appendix 1.

Technical Security

The Three Saints Academy technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site at Rainford High School,
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT Technician and will be reviewed, at least annually, by the Online Safety Group
- all users (adults and pupils) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by the IT Technician who will keep an up-to-date record of users and their usernames.
- the master account passwords for the school systems are kept in a secure place, e.g. school safe**.**
- The IT Technician is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- users to report any actual/potential technical incident/security breach to the Agilisys IT technician, any actions required are logged on the Agilisys Service Desk and acted upon accordingly
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices 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 endpoint (anti-virus) software.
- an AUP is in place for the provision of temporary access of 'guests', (e.g., trainee teachers, supply teachers, visitors) onto the school systems
- an AUP policy is in place regarding the extent of personal use that users (staff / learners / community users) and their family members are allowed on school devices that may be used out of school
- an AUP is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices
- an AUP is in place regarding the use of removable media (e.g., memory sticks/CDs/DVDs) by users on school devices.
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.

Mobile technologies

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

The Trust has considered the possible issues and risks. These may include:

- security risks in allowing connections to your school network
- filtering of personal devices
- breakages and insurance
- access to devices for all learners
- avoiding potential classroom distraction
- network connection speeds, types of devices
- charging facilities
- total cost of ownership.

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

The school allows:

	School devices			**Personal devices**		
	School owned for individual use	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**Yes**	**Yes/No**	**Yes/No**	**Yes/No**
Full network access	Yes	Yes	Yes	No	Yes/No	No
Internet only	**No**	**No**	**No**	**No**	**Yes/No**	**Yes/No**
No network access	**No**	**No**	**No**	**Yes**	**Yes/No**	**No**

[1] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

School owned/provided devices:

- *to whom they will be allocated*
- *where, when and how their use is allowed – times/places/in/out of school (n.b. the need for some areas to be clearly identified as mobile free zones)*
- *if personal use is allowed*
- *levels of access to networks/internet (as above)*
- *management of devices/installation of apps/changing of settings/monitoring*
- *network/broadband capacity*
- *technical support*
- *filtering of devices*
- *access to cloud services*
- *use on trips/events away from school*
- *data protection*
- *taking/storage/use of images*
- *exit processes, what happens to devices/software/apps/stored data if user leaves the school*
- *liability for damage*
- *staff training.*

All school owned mobile devices are filtered in the same way as all school computing devices via School Protect: Webscreen. 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 (DSL). 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, IChat 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 (DSL) has the right to take and examine users' devices in the case of misuse as detailed in the school Behaviour and Relationships Policy.

- Personal mobile phones are not to be used to take and store photographs of pupils even if for school use.

Social media

See Trust Social Media Code of Conduct

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this. This is to be read in conjunction with the Three Saint's Academy Acceptable Use Agreement and Social Media Policy.

All schools in The Three Saints Academy have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The schools within The Three Saints Academy Trust provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk
- guidance for learners, parents/carers

The Three Saints Academy staff should ensure that:

- no reference should be made in social media to pupils, parents/carers or Three Saints Academy 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 Trust.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

Where there are Three Saints Academy schools' social media accoutns established, there should be:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- 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, 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 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 school permits reasonable and appropriate access to personal social media sites during school hours*

Monitoring of public social media

- As part of active social media engagement, the school may 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
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by the IT Lead and Agilisys to ensure compliant the social media, data protection, communications, digital image and video policies.

Digital and video images

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

The Three Saints Academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.

- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images**.**
- staff/volunteers must be aware of those pupils whose images must not be taken/published.
- pupils and staff are not permitted to use personal portable media for storage of images. Images should only be taken on school devices.
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that pupils are appropriately dressed
- pupils must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with Online Safety Policy
- pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- written permission from parents or carers will be obtained annually before photographs of pupils are taken for use in school or published on the school website/social media**.** (Permission is not required for images taken solely for internal purposes)
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored on the school's network in line with the school retention policy
- pupils' work can only be published with the permission of the learner and parents/carers.
- The IT lead in liaison with Agilisys is responsible for the deletion of images no longer in use by the school or if a member of staff or pupil has left the school.

CCTV/Webcams

- Some schools in the Trust have 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 (DSL) or their nominated Deputy and the Police.

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters
- Other correspondence

The school website is managed/hosted by (amend/delete as appropriate*

TSA and SMT is managed in-house and hosted by 123-Reg

STA is managed in-house and hosted by e4education

SMI is managed in-house and hosted by 123-Reg.

The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where pupil work, images or videos are published, their identities are protected, and full names are not published.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The Three Saints Academy:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals

- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected.
- device will be password protected.
- device will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

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
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices**.**
- 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, a secure email account (where appropriate), and secure password protected devices.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and the School Committee
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate

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 online 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.

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:

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.

Appendices

Appendix 1

Filter and Monitoring Standards

Appendix 2

Trust Acceptable User Policy (Staff)

Acceptable User Policy (Pupil) add link

Appendix 3

Responding to Incidents of Misuse – flowchart

Appendix 4

Record of reviewing devices/internet sites

Appendix 5

Trust Privacy Notice Pupils

Trust Privacy Notice General

Appendix 6

Legislation

Appendix 7

Links to other organisations or documents

Appendix 8

Glossary of Terms

Appendix 1 – Filtering and Monitoring Standards

IDENTIFY AND ASSIGN ROLES AND RESPONSIBILITY TO MANAGE FILTERING AND MONITORING SYSTEM	
DfE GUIDANCE	**TRUST/SCHOOL EVIDENCE**
The importance of meeting the standard Schools and colleges should provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material. Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. It's important that the right people are working together and using their professional expertise to make informed decisions	The Chair/Safeguarding school committee member is responsible for ensuring standards are met. During safeguarding briefings with the DSL they will discuss any actions arising from the 360 degree safe audit. They also have a Safeguarding strategy briefing document with prompts of what to look for in line with the UK Council for Internet Safety guidance for Governing Boards and will speak with a group of pupils to capture pupil voice. The Headteacher/DSL is responsible for ensuring standards are met. The Trust's IT provider Agilisys monitors and controls the firewall and internet filtering system by utilising the ADEPT Education filtering system on the LGfL network. The Trust provides additional filtering and monitoring via IMPERO to enable all staff to monitor IT usage. School Protect: Webscreen – default list using pre-defined system bundles is in place, additional access rights such as Twitter can be enabled for defined groups using this system following authorisation from the CEO/Headteacher. Groups/individuals with additional access rights is discussed when reviewing the 360 degree safe audit and reviewed and updated as necessary.

	IMPERO has an advanced policy system which uses pre-defined lists updated automatically. As part of the 360 degree safe annual audit and online safety group meeting, incidents and alerts are reviewed in order that provision can be assessed on its effectiveness and any actions required such as filtering system modifications or curriculum implications. TRUST annual audit monitors if the 360 degree safe audit has been undertaken. The Headteacher discusses any actions from the Trust audit with the Chair of the School Committee School Protect: Webscreen scheduled reports are issued to Headteachers. IT technicians monitor IMPERO daily alerts and Headteachers receive automatic alerts that are categorised as “severe” along with the Trust’s Director of Safeguarding & Attendance. All alerts are monitored, those which are deemed **not** false positive are investigated and recorded on CPOMS. IMPERO alert capture reports are scheduled for Headteachers to ensure all have been monitored and actioned accordingly. IT technician undertakes spot checks of IMPERO usage by staff during lessons and provides a report to the headteachers at least half termly and actions taken accordingly by the Headteacher. Trust Annual audit monitors if spot check reports have taken place and actioned accordingly. Staff and school committee members have been trained regarding online safety on

	induction and undertake annual training. They receive IMPERO training and guidance regularly. Additional briefings are provided as part of update safeguarding briefings should issues arise. Staff are aware and trained to report concerns via the CPOMS safeguarding system. Children's views are sought regularly and fed into the-online safety group.
REVIEW YOUR FILTERING AND MONITORING PROVISION AT LEAST ANNUALLY	
DfE GUIDANCE	**TRUST/SCHOOL EVIDENCE**
The importance of meeting the standard For filtering and monitoring to be effective it should meet the needs of your pupils and staff, and reflect your specific use of technology while minimising potential harms. To understand and evaluate the changing needs and potential risks of your school or college, you should review your filtering and monitoring provision, at least annually. Additional checks to filtering and monitoring need to be informed by the review process so that governing bodies and proprietors have assurance that systems are working effectively and meeting safeguarding obligations.	A 360 degree SAFE audit tool is completed annually and its results shared with the Chair of the School Committee. TRUST annual audit monitors if the 360 degree safe audit has been undertaken. The Headteacher discusses any actions from the Trust audit with the Chair of the School Committee As part of the 360 degree safe annual audit and online safety group meeting, incidents and alerts are reviewed in order that provision can be assessed on its effectiveness and any actions required such as filtering system modifications or curriculum implications. Actions from any safeguarding issue that arises may also require reviewing and updating provision sooner than the annual review. Online safety incidents are reported to the school committee. School committee member responsible for safeguarding meets with the DSL and also

	meets with pupils to discuss safeguarding issues and review practice. **Technical requirements** The Trust's IT provider Agilisys monitors and controls the firewall and internet filtering system by utilising the ADEPT Education filtering system on the LgFL network. The Trust provides additional filtering and monitoring via IMPERO to enable all staff to monitor IT usage. IMPERO alert reports identify risk categories. CPOMS reports identifies risk categories. School are aware of their contextual safeguarding issues and have a matrix of vulnerability which identifies the risk profile of their pupils. Online safety is delivered throughout the school curriculum not just part of computing curriculum and enhanced further through PHSE, RSE themed days and weeks as well as signposted links through the school website and in conjunction with DfE Teaching Online Safety in Schools January 2023 and Education for a Connected World Framework School Protect: Webscreen filtering checks are completed by the IT technician monthly using the SWGfL testing tool and reported to the Headteacher/DSL. School Protect: Webscreen – default list using pre-defined system bundles is in place, additional access rights such as Twitter can be enabled for defined groups using this system following authorisation from the

	CEO/Headteacher. Groups/individuals with additional access rights is discussed when reviewing the 360 degree safe audit and reviewed and updated as necessary. Spot checks of staff having IMPERO open is undertaken by the IT technician and reported to the Headteacher at least half termly with action taken were necessary. Alerts are monitored daily. Alert MONITORING reports are scheduled weekly. Concerns are logged on CPOMS and all staff are trained.
YOUR FILTERING SYSTEM SHOULD BLOCK HARMFUL AND INAPPROPRIATE CONTENT, WITHOUT REASONABLY IMPACTING TEACHING AND LEARNING	
DfE GUIDANCE	**TRUST/SCHOOL EVIDENCE**
The importance of meeting the standard An active and well managed filtering system is an important part of providing a safe environment for pupils to learn. No filtering system can be 100% effective. You need to understand the coverage of your filtering system, any limitations it has, and mitigate accordingly to minimise harm and meet your statutory requirements in Keeping children safe in education (KCSIE) and the Prevent duty. An effective filtering system needs to block internet access to harmful sites and inappropriate content. It should not: • unreasonably impact teaching and learning or school administration • restrict students from learning how to assess and manage risk themselves	School Protect: Webscreen – default list using pre-defined system bundles is in place, additional access rights such as Twitter can be enabled for defined groups using this system following authorisation from the CEO/Headteacher. Groups/individuals with additional access rights is discussed when reviewing the 360 degree safe audit and reviewed and updated as necessary. IMPERO has an advanced policy system which uses pre-defined lists updated automatically. All incidents are reported on CPOMS by staff and actioned accordingly.

YOU SHOULD HAVE EFFECTIVE MONITORING STRATEGIES THAT MEET THE SAFEGUARDING NEEDS OF YOUR SCHOOL OR COLLEGE	
DfE GUIDANCE	**TRUST/SCHOOL EVIDENCE**
The importance of meeting the standard Monitoring user activity on school and college devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software. Monitoring allows you to review user activity on school and college devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome. Your monitoring strategy should be informed by the filtering and monitoring review. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include: • physically monitoring by staff watching screens of users • live supervision by staff on a console with device management software • network monitoring using log files of internet traffic and web access • individual device monitoring through software or third-party services	The Chair/Safeguarding school committee member (NAME) is responsible for ensuring standards are met. During safeguarding briefings with the DSL they will discuss any actions arising from the 360 degree safe audit. They also have a Safeguarding strategy briefing document with prompts of what to look for in line with the UK Council for Internet Safety guidance for Governing Boards and will speak with a group of pupils to capture pupil voice. The Headteacher/DSL (NAME) is responsible for ensuring standards are met. The Trust's IT provider Agilisys monitors and controls the firewall and internet filtering system by utilising the ADEPT Education filtering system on the LGfL network. The Trust provides additional filtering and monitoring via IMPERO to enable all staff to monitor IT usage. School Protect: Webscreen – default list using pre-defined system bundles is in place, additional access rights such as Twitter can be enabled for defined groups using this system following authorisation from the CEO/Headteacher. Groups/individuals with additional access rights is discussed when reviewing the 360 degree safe audit and reviewed and updated as necessary. IMPERO has an advanced policy system which uses pre-defined lists updated automatically.

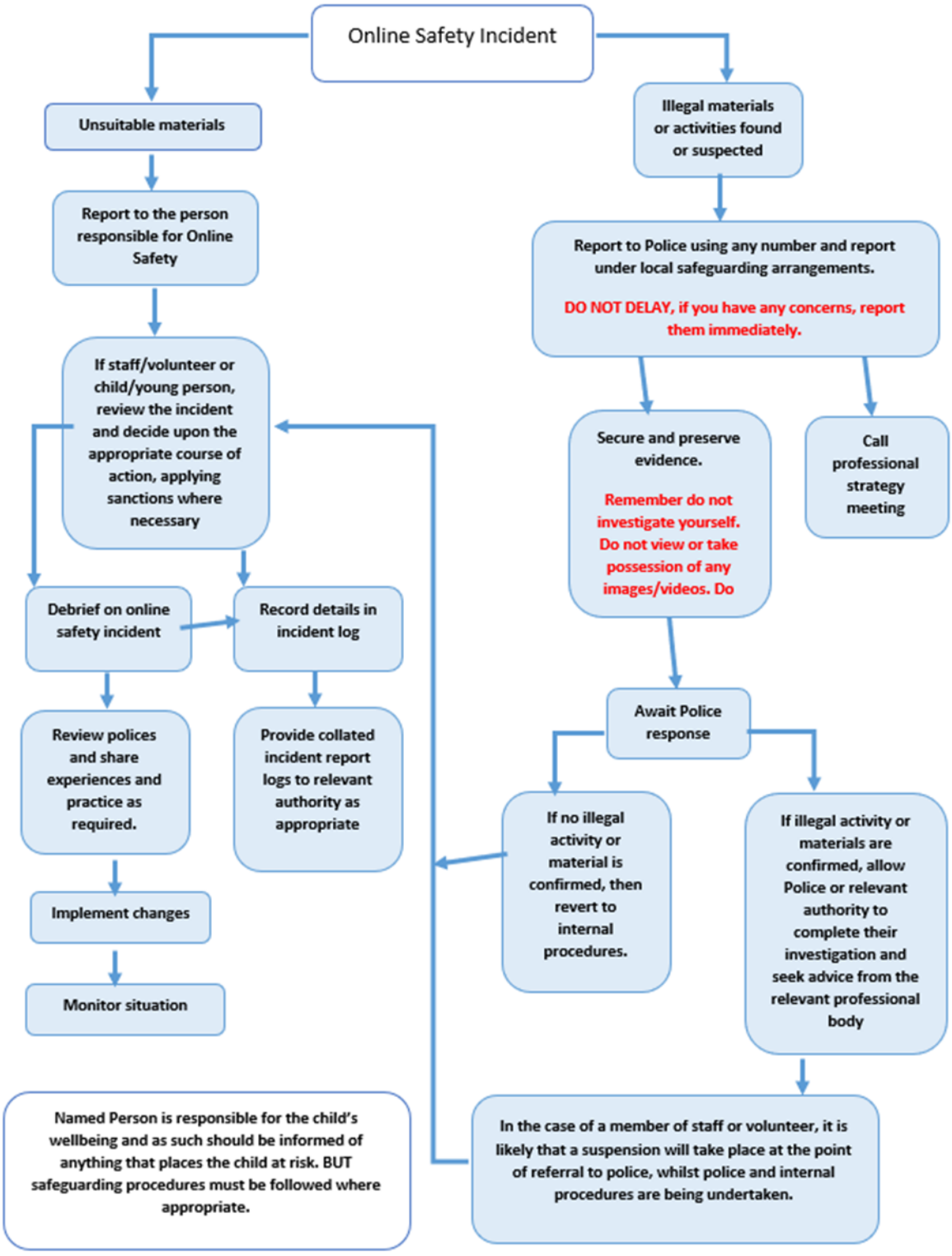
	As part of the 360 degree safe annual audit and online safety group meeting, incidents and alerts are reviewed in order that provision can be assessed on its effectiveness and any actions required such as filtering system modifications or curriculum implications. TRUST annual audit monitors if the 360 degree safe audit has been undertaken. The Headteacher discusses any actions from the Trust audit with the Chair of the School Committee School Protect: Webscreen scheduled reports are issued to Headteachers. IT technicians monitor IMPERO daily alerts and Headteachers receive automatic alerts that are categorised as "severe" along with the Trust's Director of Safeguarding & Attendance. All alerts are monitored, those which are deemed **not** false positive are investigated and recorded on CPOMS. IMPERO alert capture reports are scheduled for Headteachers to ensure all have been monitored and actioned accordingly. IT technician undertakes spot checks of IMPERO usage by staff during lessons and provides a report to the headteachers at least half termly and actions taken accordingly by the Headteacher. Trust Annual audit monitors if spot check reports have taken place and actioned accordingly. Staff and school committee members have been trained regarding online safety on induction and undertake annual training. They receive IMPERO training and guidance regularly. Additional briefings are provided as

	part of update safeguarding briefings should issues arise. Staff are aware and trained to report concerns via the CPOMS safeguarding system. Cyber Security training is part of the SMARTLOG training package that all staff and Chair of School Committees complete.

Appendix 2 – AUPs

Appendix 3

Responding to incidents of misuse – flow chart



Appendix 4

Record of reviewing devices / internet sites (responding to incidents of misuse) staff only all pupil incidents logged on CPOMS.

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 – PRIVACY NOTICE

Appendix 6 - Legislation

Schools 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.

A useful summary of relevant legislation can be found at: Report Harmful Content: Laws about harmful behaviours

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.

Schools 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:

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 learners 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.

(see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/learnersupport/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 – Links to other organisations or documents

This policy should be read in conjunction with

Staff Code of Conduct
Social Media Code of Conduct
Data Protection Policy
Safeguarding and Child Protection Policy
Behaviour and Relationships Policy
Anti-bullying Policy
Anti-Extremism Policy
Curriculum Policies: Computing, PHSE/RSE

Further guidance:

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/
Harmful Sexual Support Service

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

Tools for Schools / other organisations

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

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

SWGfL 360 Groups – online safety self review tool for organisations working with children

SWGfL 360 Early Years - online safety self review tool for early years organisations

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

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

Department for Education: Teaching Online Safety in Schools

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guides for Organisations

IRMS - Records Management Toolkit for Schools

ICO Guidance on taking photos in schools

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/Cyber-security

UKSIC – Appropriate Filtering and Monitoring

SWGfL Safety & Security Resources

Somerset - Questions for Technical Support

SWGfL - Cyber Security in Schools.

NCA – Guide to the Computer Misuse Act

NEN – Advice and Guidance Notes

Working with parents and carers

SWGfL – Online Safety Guidance for Parents & Carers

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

Childnet – Trust Me

Research

Ofcom –Media Literacy Research

Ofsted: Review of sexual abuse in schools and colleges

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Appendix 8 – Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	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.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
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
MAT	Multi Academy Trust
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 online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety

VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework