



# Knights Templar Community Church School and Nursery

*Work at it with all your heart*

Head Teacher: Mrs Laura Weaver, BA Hons QTS

# Online Safety Policy

Date Approved by the Headteacher	Review Period	Date to be reviewed
March 2025	Annual	March 2026

*This policy applies to all members of the school community, including staff, learners, volunteers, parents and carers, visitors, community users who have access to and are users of the school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site.*

This Online Safety Policy outlines the commitment of Knights Templar Community Church School and Nursery to safeguard members of our school community online in accordance with statutory guidance and best practice.

Knights Templar Community Church School & Nursery will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

### **Policy development, monitoring and review**

This Online Safety Policy has been developed by the **Online Safety Group**. The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives.

The Online Safety Group has the following members

- Designated Safeguarding Lead
- Online Safety Lead- Computing Lead
- Online Safety governor
- technical staff
- Digital Leaders
- parents/carers

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for development, monitoring and review.

This Online Safety Policy was approved by the school governing body on:	March 2024
The implementation of this Online Safety Policy will be monitored by:	Ollie Armitage, Online Safety Co-ordinator
Monitoring will take place at regular intervals:	This will occur at the end of each term.
The governing body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	This will occur at the end of each term.

<p>The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:</p>	<p>6th November 2024</p>
<p>Should serious online safety incidents take place, the following external persons/agencies should be informed:</p>	<p>LADO 03001232224 Somerset Education Safeguarding Leads <a href="mailto:educationsafeguardinglead@somerset.gov.uk">educationsafeguardinglead@somerset.gov.uk</a> Police</p>

## Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using

- logs of reported incidents
- Filtering and monitoring logs
- internal monitoring data for network activity
- surveys/questionnaires of:
  - learners
  - parents and carers
  - staff

## Policy and Leadership

### Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of the community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

## **Headteacher and senior leaders**

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in *Keeping Children Safe in Education*.
- The headteacher and all the members of the senior leadership team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff- this relates to our flowchart.
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Coordinator, IT provider/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/senior leaders 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.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead compiled by the Online Safety Coordinator.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and the Online Safety Coordinator and IT service providers in all aspects of filtering and monitoring.

## **Governors**

The DfE guidance “*Keeping Children Safe in Education*” states:

“Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children’s welfare .... this includes ... online safety”

“Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)”

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e by asking the questions posed in the UKCIS document “*Online Safety in Schools and Colleges – questions from the Governing Body*”.

This review will be carried out by the Online Safety Group, which includes the Online Safety Governor, whose members will receive regular information about online safety incidents and monitoring reports. The Online Safety Group will hold

- regular meetings
- will regularly receive (collated and anonymised) reports of online safety incidents

- check that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- ensure that the filtering and monitoring provision is reviewed and recorded, at least termly. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) – in-line with the DfE Filtering and Monitoring Standards
- report to governors
- receive (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- the governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

### **Designated Safety Lead (DSL)**

Keeping Children Safe in Education states that:

*“ The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder’s job description.”*

*They (the DSL) “are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college”*

*They (the DSL) “can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online”*

**The DSL will:**

- hold the lead responsibility for online safety, within their safeguarding role.
- receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety coordinator and governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings
- report regularly to headteacher and other members of the senior leadership team

- *be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded*
- *liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)*

### **The Online Safety Coordinator**

*The Online Safety Coordinator will:*

- *lead the Online Safety Group*
- *work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)*
- *receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments*
- *have a leading role in establishing and reviewing the school online safety policies/documents*
- *promote an awareness of and commitment to online safety education / awareness raising across the school and beyond*
- *liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated*
- *ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents*
- *provide (or identify sources of) training and advice for staff/governors/parents/carers/learners*
- *liaise with (school/local authority, technical staff, pastoral staff and support staff (as relevant)*
- *receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:*
  - *content*
  - *contact*
  - *conduct*
  - *commerce*

### **Curriculum Leads**

*Curriculum Leads will work with the DSL/OSC to develop a planned and coordinated online safety education programme eg Active BYTES online safety curriculum.*

*This will be provided through:*

- *a discrete programme and embedded across the curriculum.*

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

## **Teaching and support staff**

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to Laura Weaver, the DSL for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are 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
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, 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 regarding these devices
- in lessons where internet use is pre-planned learners are 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, there is regard to national safeguarding guidance and local safeguarding policies
- there is 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

## **Knights Templar IT Provider SWGfL and Computeam**

The DfE Filtering and Monitoring Standards says:

*“Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider.”*

*“Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support.”*

*“The IT service provider should have technical responsibility for:*

- o maintaining filtering and monitoring systems*
- o providing filtering and monitoring reports*
- o completing actions following concerns or checks to systems”*

*“The IT service provider should work with the senior leadership team and DSL to:*

- o procure systems*
- o identify risk*
- o carry out reviews*
- o carry out checks”*

**Both SWgFL and Computeam are responsible for ensuring that:**

- they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority or other relevant body.
- there is clear, safe, and managed control of user access to networks and devices
- 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
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to Laura Weaver, the DSL, for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring systems are implemented and regularly updated as agreed in school policies

### **Learners**

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy- this includes personal devices
- should 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.

- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

## **Parents and carers**

Knights Templar Community Church School and Nursery will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed)

## **Community users**

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

## **Online Safety Group**

Members of the Online Safety Group will assist the DSL/OSC with:

- the production/review/monitoring of the school Online Safety Policy/documents
- the production/review/monitoring of the school filtering policy 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 learners to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

- An Online Safety Group terms of reference can be found in the appendices.

## **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**

### *Online Safety Policy*

The DfE guidance “Keeping Children Safe in Education” states:

“Online safety and the school or college’s approach to it should be reflected in the child protection policy”

### **The school 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 learners in the digital world
- describes how the school will help prepare learners 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
- is published on the school website.

## **Acceptable use**

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 handbook
- posters/notices around where technology is used
- communication with parents/carers

- built into education sessions
- school website

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

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:	<p><b>Any illegal activity for example:</b></p> <ul style="list-style-type: none"> <li>• Child sexual abuse imagery*</li> <li>• Child sexual abuse/exploitation/grooming</li> <li>• Terrorism</li> <li>• Encouraging or assisting suicide</li> <li>• Offences relating to sexual images i.e., revenge and extreme pornography</li> <li>• Incitement to and threats of violence</li> <li>• Hate crime</li> <li>• Public order offences - harassment and stalking</li> <li>• Drug-related offences</li> <li>• Weapons / firearms offences</li> <li>• Fraud and financial crime including money laundering</li> </ul> <p><i>N.B. Schools should refer to guidance about dealing with self-generated images/sexting - <a href="#">UKSIC Responding to and managing sexting incidents</a> and <a href="#">UKCIS - Sexting in schools and colleges</a></i></p>					X
Users shall not undertake activities that might be classed as cyber-	<ul style="list-style-type: none"> <li>• 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)</li> </ul>					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
crime under the Computer Misuse Act (1990)	<ul style="list-style-type: none"> <li>Gaining unauthorised access to school networks, data and files, through the use of computers/devices</li> <li>Creating or propagating computer viruses or other harmful files</li> <li>Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)</li> <li>Disable/Impair/Disrupt network functionality through the use of computers/devices</li> <li>Using penetration testing equipment (without relevant permission)</li> </ul> <p><i>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. The National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – further information <a href="#">here</a></i></p>					
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	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				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:	Staff and other adults		Learners					
	<i>To do in consultation</i>							
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff
Online gaming	★				★			

Online shopping/commerce			★		★			
File sharing			★		★			
Social media	★				★			
Messaging/chat			★		★			
Entertainment streaming e.g. Netflix, Disney+			★		★			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok			★		★			
Mobile phones may be brought to school			★					★
Use of mobile phones for learning at school	★				★			
Use of mobile phones in social time at school		★			★			
Taking photos on mobile phones/cameras				★				★
Use of other personal devices, e.g. tablets, gaming devices	★				★			
Use of personal e-mail in school, or on school network/wi-fi			★		★			
Use of school e-mail for personal e-mails			★		★			

When using communication technologies, the school 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 learners 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 should be 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 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 learners.

## 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 learners. 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:

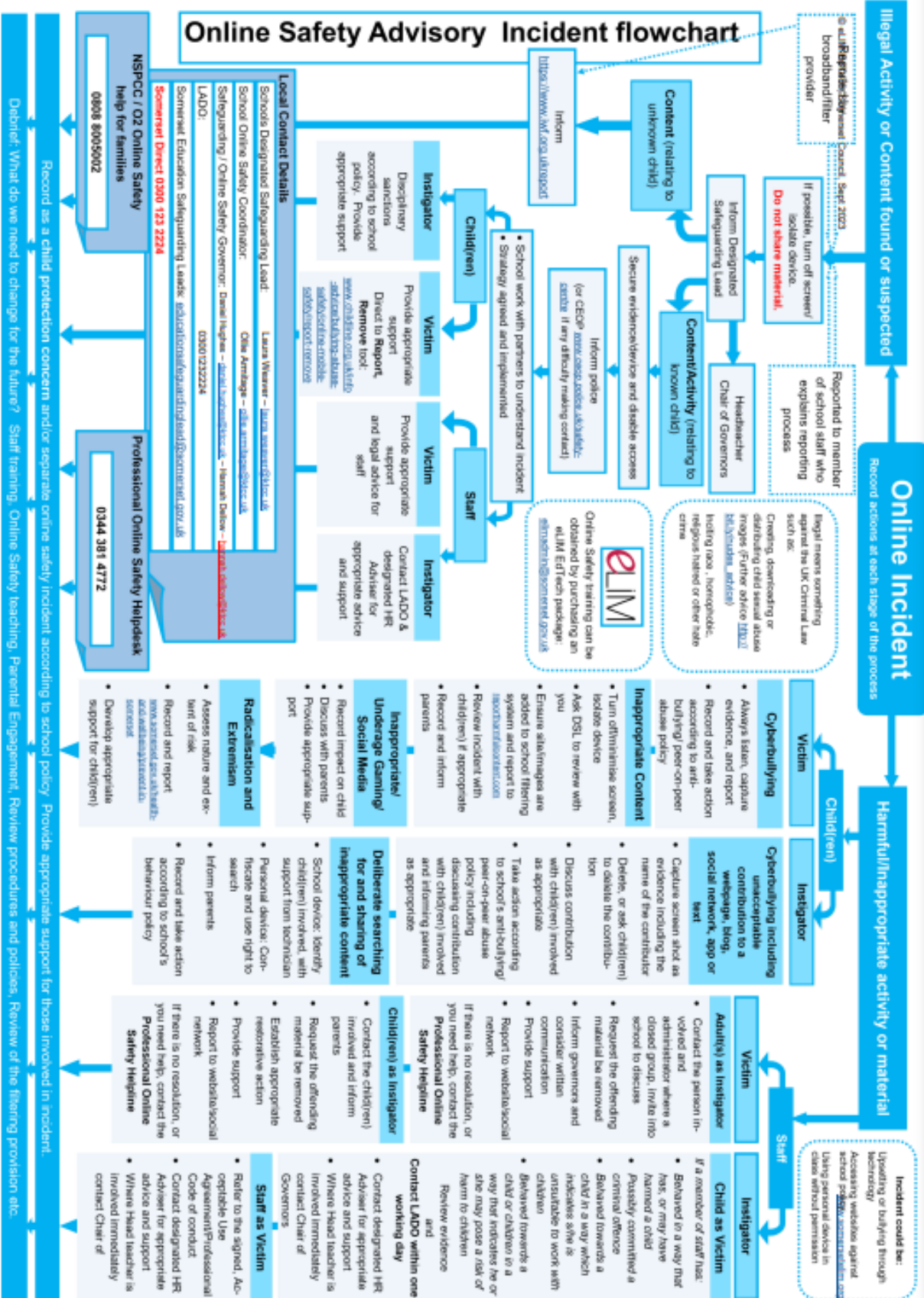
- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware 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 Designated Safeguarding Lead, Online Safety Coordinator 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 the incident must be escalated through the agreed school safeguarding procedures. This may include.
  - Non-consensual images
  - Self-generated images
  - Terrorism/extremism
  - Hate crime/ Abuse
  - Fraud and extortion
  - Harassment/stalking
  - Child Sexual Abuse Material (CSAM)
  - Child Sexual Exploitation Grooming
  - Extreme Pornography
  - Sale of illegal materials/substances
  - Cyber or hacking offences under the Computer Misuse Act
  - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority.
- 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 learners 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*
  - *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 on the reporting log template.*
- *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 relevant)*
- *learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:*
  - *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
  - *staff, through regular briefings*
  - *learners, through assemblies/lessons*
  - *parents/carers, through newsletters, school social media, website*
  - *governors, 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.*

*Knights Templar Community Church School Online Safety Advisory Incident flowchart:*



## Online Safety Advisory Incident flowchart

### Local Contact Details

Schools Designated Safeguarding Lead: [Laura Wheeler - \[laura.wheeler@hinc.lincs.gov.uk\]\(mailto:Laura.Wheeler@laura.wheeler@hinc.lincs.gov.uk\)](mailto:Laura.Wheeler@laura.wheeler@hinc.lincs.gov.uk)

School Online Safety Coordinator: [Oliver Average - \[oliver.average@hinc.lincs.gov.uk\]\(mailto:Oliver.Average@oliver.average@hinc.lincs.gov.uk\)](mailto:Oliver.Average@oliver.average@hinc.lincs.gov.uk)

Safeguarding / Online Safety Governor: [Debra Hughes - \[debra.hughes@hinc.lincs.gov.uk\]\(mailto:Debra.Hughes@debra.hughes@hinc.lincs.gov.uk\)](mailto:Debra.Hughes@debra.hughes@hinc.lincs.gov.uk)

LADO: [0300 1232224](mailto:0300 1232224)

Somerset Education Safeguarding Lead: [educationalguardians@somerset.gov.uk](mailto:educationalguardians@somerset.gov.uk)

Somerset Direct: [0300 123 2224](tel:0300 123 2224)

### NSPCC / Q2 Online Safety help for families

[0800 8005002](tel:0800 8005002)

### Professional Online Safety Helpline

[0344 381 4772](tel:0344 381 4772)

### Radicalisation and Extremism

- Assess nature and extent of risk
- Record and report non-urgent concerns to [radicalisation@hinc.lincs.gov.uk](mailto:radicalisation@hinc.lincs.gov.uk)
- Develop appropriate support for children/instigator

### Deliberate searching for and sharing of inappropriate content

- School device: Identify children/ involved, with support from technician
- Personal device: Contact and use right to search
- Inform parents
- Record and take action according to school's behaviour policy

### Children

**Instigator**

- Disciplinary sanctions according to school policy. Provide appropriate support

**Victim**

- Provide appropriate support
- Direct to Report, Remove tool: [www.onlinesafety.gov.uk](http://www.onlinesafety.gov.uk)
- Remove tool: [report@onlinesafety.gov.uk](mailto:report@onlinesafety.gov.uk)

**Staff**

- Provide appropriate support and legal advice for staff

**Instigator**

- Contact LADO & designated HR Adviser for appropriate advice and support

### Inappropriate/ Underage Gaming/ Social Media

- Record impact on child
- Discuss with parents
- Provide appropriate support

### Child(ren) as Instigator

- Contact the children/ involved and inform parents
- Request the offending material be removed
- Establish appropriate restorative action
- Provide support
- Report to web/social network

### Staff as Victim

- Refer to the signed, Acceptable Use Agreement/Professional Code of conduct
- Contact designated HR Adviser for appropriate advice and support
- Where Head teacher is involved immediately contact Chair of Governors

### Contact LADO within one working day

- Contact designated HR Adviser for appropriate advice and support
- Where Head teacher is involved immediately contact Chair of Governors

## School actions

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

## Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to Deputy Head	Refer to Headteacher/DSL	Refer to Police/Childrens Social Care	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	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
Corrupting or destroying the data of other users.		X	X			X		X	X
Sending an e-mail, text or message that is regarded as		X	X		X	X		X	X

offensive, harassment or of a bullying nature									
Unauthorised downloading or uploading of files or use of file sharing.		X	X			X		X	X
Using proxy sites or other means to subvert the school's filtering system.		X	X		X	X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident.		X	X		X	X		X	
Deliberately accessing or trying to access offensive or pornographic material.		X	X		X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		X	X	X	X	X	X	X	X
Unauthorised use of digital devices (including taking images)		X	X			X		X	X
Unauthorised use of online services		X	X			X		X	X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X	X			X		X	

Continued infringements of the above, following previous warnings or sanctions.		X	X			X	X	X	X
---	--	---	---	--	--	---	---	---	---

### Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher/ DSL	Refer to local authority/HR	Refer to Police	Refer to LA / Technical Support Staff <i>for action re filtering etc</i>	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				X
Deliberate actions to breach data protection or network security rules.		X	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	X					X
Unauthorised downloading or uploading of files or file sharing		X						X
Breaching copyright or licensing regulations.		X	X					X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the		X						X

school network, using another person's account.								
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X				X
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers		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			X		X
Actions which could compromise the staff member's professional standing		X						X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		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

### **Online Safety Education Programme**

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of our school's online safety provision.

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'."*

Keeping Children Safe in Education states:

*"Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum ..."*

Online safety is a focus in all areas of the curriculum and staff will reinforce online safety messages across the curriculum.

The online safety curriculum is 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. Active BYTES and the SWGfL Project Evolve 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 needs 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; English etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme is accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- learners 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. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990.
- 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 learners 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 learners are allowed to freely search the internet, staff are extra vigilant in supervising the learners and monitoring the content of the websites the young children visit
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

### **Contribution of Learners**

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

- mechanisms to canvass learner feedback and opinion.
- appointment of digital leaders
- the Online Safety Group has learner representation
- learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns
- learners 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. An audit of the online safety training needs of all staff will be carried out regularly
- 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 Coordinator and/or Designated Safeguarding Lead will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / 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 Designated Safeguarding Lead or Online Safety Coordinator will provide advice/guidance/training to individuals as required.

## **Governors**

Governors will take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority or other relevant organisation (e.g., SWGfL)
- participation in school training / information sessions for staff or parents eg assemblies

A higher level of training will be made available to the Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

## **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 school 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 learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- letters, newsletters, website,
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. SWGfL; [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/); [www.childnet.com/parents-and-carers](http://www.childnet.com/parents-and-carers)
- Sharing good practice with other schools in clusters and or the local authority.

### **Adults and Agencies**

The school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- online safety messages targeted towards families and relatives.
- providing family learning courses in use of digital technologies and online safety
- providing online safety information via their website and social media for the wider community
- supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision

### **Technology**

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school ensures that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

## Filtering & Monitoring

The DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" states:

*"It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the ... risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified..."*

*The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards..."*

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed termly and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

The filtering and monitoring provision is reviewed termly by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

- checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement the Online Safety Group and the Headteacher in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced

## Filtering

- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre

### Appropriate filtering.

- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL 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, recognising that no system can be 100% effective
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- younger learners will use child friendly/age-appropriate search engines e.g. [SWGfL Swiggle](#)
- 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.

### **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.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- 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.

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 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 to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

## Technical Security

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

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- 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 service provider and will be reviewed, at least annually, by the SLT/Online Safety Group
- password policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)
- the security of their username and password and must not allow other users to access the systems using their log on details.
- all users 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.
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for school systems are kept in a secure place, e.g. school safe.
- there is a risk-based approach to the allocation of learner usernames and passwords.
- 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
- 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 software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- The School Online Coordinator 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.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network

- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place
- guest users are provided with appropriate access to school systems based on an identified risk profile eg supply teachers.

## **Mobile Technologies**

*The DfE guidance “Keeping Children Safe in Education” states:*

*“The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.*

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

Our school allows:

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

### School owned/provided devices:

- all school devices are managed through the use of Mobile Device Management software
- there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed
- any designated mobile-free zone is clearly signposted
- personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.
- the use of devices on trips/events away from school is clearly defined and expectation are well-communicated.
- liability for damage aligns with current school policy for the replacement of equipment.
- education is in place to support responsible use.

### Personal devices:

- where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storage should be made available.
- use of personal devices for school business is defined in the acceptable use policy and staff handbook. Personal devices commissioned onto the school network are segregated effectively from school-owned systems

- *the expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.*
- *liability for loss/damage or malfunction of personal devices is clearly defined*
- *there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements*
- *education about the safe and responsible use of mobile devices is included in the school online safety education programmes*

## **Social media**

*The school 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*

## **School staff ensure that:**

- *No reference should be made in social media to learners, parents/carers or school staff.*
- *they do not engage in online discussion on personal matters relating to members of the school community.*
- *personal opinions should not be attributed to the school.*
- *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*

## **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, or impacts on, the school it must be made clear that the member*
- *of staff is not communicating on behalf of the school 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 a senior leader and the Online Safety Coordinator to ensure compliance with the social media and data protection, policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline. .

### **Digital and video images**

The school 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. Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education
- 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 learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images

- *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 learners are appropriately dressed*
- *learners must not take, use, share, publish or distribute images of others without their permission*
- *photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy*
- *learners' 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 before photographs of learners are taken for use in school or published on the school website/social media. (*
- *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 in line with the school retention policy*
- *learners' work can only be published with the permission of the learner and parents/carers.*

## **Online Publishing**

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

- *Public-facing website*
- *Online newsletters*

*The school website is managed/hosted by Primary Site.. 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 learner work, images or videos are published, their identities are protected, and full names are not published.*

*The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.*

*The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.*

## *Data Protection*

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

*The school:*

- 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. Procedures should be in place to enable staff to work from home (i.e. VPN access to the school network, or a work laptop provided).
- 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 Governors*
- 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*
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.*

*:*

## *School Online Safety Policy Appendices*

### *Appendices*

- *Learner Acceptable Use Agreement Template – for younger learners (Foundation/KS1)*
- *Parent/Carer Permissions*
- *Staff (and Volunteer) Acceptable Use Policy Agreement Template*
- *Online Safety Group Terms of Reference Template*
- *Responding to incidents of misuse – flow chart*
- *Record of reviewing devices/internet sites (responding to incidents of misuse)*
- *Reporting Log*
- *Training Needs Audit Log*
- *Technical Security Policy Template (including filtering and passwords)*
- *School Online Safety Policy Template: Electronic Devices – Searching Screening and Confiscation (new DfE guidance from September 2022)*

### *Legislation*

*Links to other organisations and resources*

### *Glossary of Terms*

# Learner Acceptable Use of Technology Policy

Technology is a great tool to support learning, find information and to communicate and share with others.

The School encourages its appropriate, effective and safe use. All users of technology in the school must agree to certain rules and will only use the equipment and software as instructed.

## My Responsibilities

I understand that the school will monitor my use of computers and other technology.

I understand that I have rights and responsibilities in using technology and will follow the agreed rules when using technology including the internet.

I understand that the school may investigate incidents that cause upset or harm taking place outside school.

I recognise if I misuse technology, it has an effect on others and consequences for me.

I will report any suspected misuse or problems to a trusted adult in the school.

I will think about the ways I use technology so that it will not negatively affect my physical or mental health.

## Online bullying

I understand that the school will not accept bullying in any form.

I will be careful to check that anything I write or say in documents, messages or online is not offensive or could cause hurt or embarrassment.

## Use of internet

I will not try to access sites that are blocked or that are unsuitable for use in school.

I will carefully check information I use for my learning.

I will report any worrying or damaging materials I come across.

## Personal mobile devices

I will only use personal mobile devices when I have permission from by my teachers.

Name \_\_\_\_\_

Signed \_\_\_\_\_

Class \_\_\_\_\_ Date \_\_\_\_\_

## Permission agreements for Knights Templar Community Church School



Name: ..... Class: .....

Please tick the boxes to show agreement:

Local visits:	
I give permission for my child to join any visit organised by the school within our locality.	
I give permission for my child to travel accompanied in a car with the Head Teacher/Deputy Head Teacher in an emergency, using a child seat if appropriate.	
<p>I know of no medical reason why he/she should not participate in routine off-site activities. It is my responsibility to inform the school if my son/daughter is unable to participate in such activities.</p> <p>I am aware that:</p> <ul style="list-style-type: none"> <li>except for visits abroad, insurance arrangements are the same as for students in school, i.e. that the Authority only provides cover against proven or agreed negligence by the Authority and its employees.</li> <li>I should consider making my own insurance arrangements for personal accident cover for my son/daughter</li> </ul>	

Recording and use of images and sound:	
I give permissions for the school to use my child's photograph in the school prospectus and other promotional publications.	
I give permission for the school to use my child's image on the school website.	
I give permission for the school to use my child's image in media reports (newspapers).	
I give permission for my child's first name to be printed alongside an image.	
I give permission for the school to publish video recordings of school activities that include my child.	
I give permission for the school to publish sound recordings of school activities that include my child.	

<i>The school can use my child's image in social media postings through the school's blogging account.</i>	
<i>The school can print my child's name in newsletters which are available on the school website.</i>	
<i>I give permission for my child's image to be included on class activity photos that are sent home.</i>	

<b>Use of the internet:</b>	
<i>I give permission for my child to use the internet for educational activities in school.</i>	

<b>First Aid:</b>	
<i>I give permission for my child to have antiseptic wipes used if required.</i>	
<i>I give permission for plasters to be used if needed.</i>	

<b>Local support:</b>	
<i>I give permission for concerns about my child to be raised with local support professionals.</i>	

Parent/Carer name ..... (please print)

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

# Knights Templar Community Church School



## Staff

### Code of Conduct

*I have read, understand and am able to work within Knights Templar Community Church School's and Knights Templar Nursery's Code of Conduct as reviewed in September 2023.*

*By signing, I am acknowledging that I have read the Keeping Children Safe in Education 2023, Part 1 document.*

### Staff Disqualification Declaration Form

*Following updated statutory guidance from the Department of Education the school is now required to ensure that all staff/volunteers are not disqualified from doing so under the Childcare (Disqualification) Regulations 2009.*

*You may be disqualified if one of the following applies:*

- You have been cautioned for, or convicted of, certain violent or sexual criminal offences against adults or children.*
- You are the subject of an Order, direction or similar in respect of childcare, including orders in respect of your own children.*
- You have had your registration refused or cancelled in relation to childcare, including orders made in respect of your own children.*

*To meet this statutory requirement, we require you to complete and sign the form below. If you are unsure of how to answer any of the questions then you should seek further guidance from the Headteacher/Chair of Governors.*

<i>Are you disqualified from caring for children?</i>	<i>Yes / No</i>
<i>Have you been barred from working in regulated activities with children?</i>	<i>Yes / No</i>

Do you have any convictions, cautions, reprimands or final warnings that are not “protected” as defined by the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (as amended in 2013)?*	Yes / No
Have your own children been subject to a child protection order?	Yes / No
Are you disqualified from private fostering?	Yes / No
Please provide further information where you have answered “yes” to any of the above questions.	

I confirm the accuracy of the above statements and will make the school aware of any changes in these circumstances, including any cautions or convictions that may affect my suitability to work at the school.

\* For existing staff this will already have been obtained through DBS checks or previous police checks. Any information disclosed will not be used to re-assess someone’s suitability for a post unless the conviction / caution or reprimand specifically impacts on your ability to carry out the role.

### **Pecuniary Interest**

The financial advisers from Somerset County Council have advised all schools to ask governors/staff if they have a ‘Pecuniary Interest’ in any person or company that may have any financial dealings with the school. This does not exclude these people but there should be a declaration of interest.

The Governing Body have defined a ‘pecuniary interest’ as a situation where the person concerned, their family (immediate and other relative) or close friends have a connection with a potential supplier, or where there is a business connection, ie common directorships/ partnerships. (For example you are related to a plumber who may be asked to work in the school or nursery.)

If you have no associations, please write ‘nil’ in the Name of Company box and sign and date the form.

Name of Company/ Person that you are associated with	Nature of Business or Interest

*Staff Acceptable Use Policy and Health and Safety Policy*

*I have read and understand the full School online safety policy and agree to use the school technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) in a responsible and professional manner as outlined in that document. I have read and understand the Health and Safety Policy.*

*Signed:*

*Name:*

*Date:*

# Knights Templar Community Church School and Nursery



*“Be the best you can be with a zest for living, a thirst for learning and a spirit of kindness.”*

Head Teacher: Mrs Laura Weaver, BA Hons QTS

## *Online Safety Group Terms of Reference*

### *1. Purpose*

*To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.*

### *2. Membership*

*The Online Safety Group has the following members*

- Designated Safeguarding Lead*
- Online Safety Lead- computer Lead*
- online safety governor*
- technical staff*
- Digital leaders learners*
- parents/carers*

*Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.*

*2.1. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.*

*2.2. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature*

*2.3. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities*

### *3. Chairperson*

*The Committee should select a suitable Chairperson from within the group. Their responsibilities include:*

- Scheduling meetings and notifying members;*
- Inviting other people to attend meetings when required*
- Guiding the meeting according to the agenda and time available;*
- Ensuring all discussion items end with a decision, action or definite outcome;*

- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

#### 4. Frequency of Meetings

Meetings shall be held once a term.

#### 5. Functions

These are to assist the DSL and OSL with the following

- To keep up to date with new developments in the area of online safety
- To review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through
  - Staff meetings
  - Learner forums (for advice and feedback)
  - Governors meetings
  - Surveys/questionnaires for learners, parents/carers and staff
  - Parents evenings
  - Website/newsletters
  - Online safety events
  - Internet Safety Day (annually held on the second Tuesday in February)
  - Other methods
- To ensure that monitoring is carried out of Internet sites used across the schools.
- To monitor filtering/change control logs (e.g. requests for blocking/unblocking sites).
- To monitor the safe use of data across the schools
- To monitor incidents involving cyberbullying for staff and learners

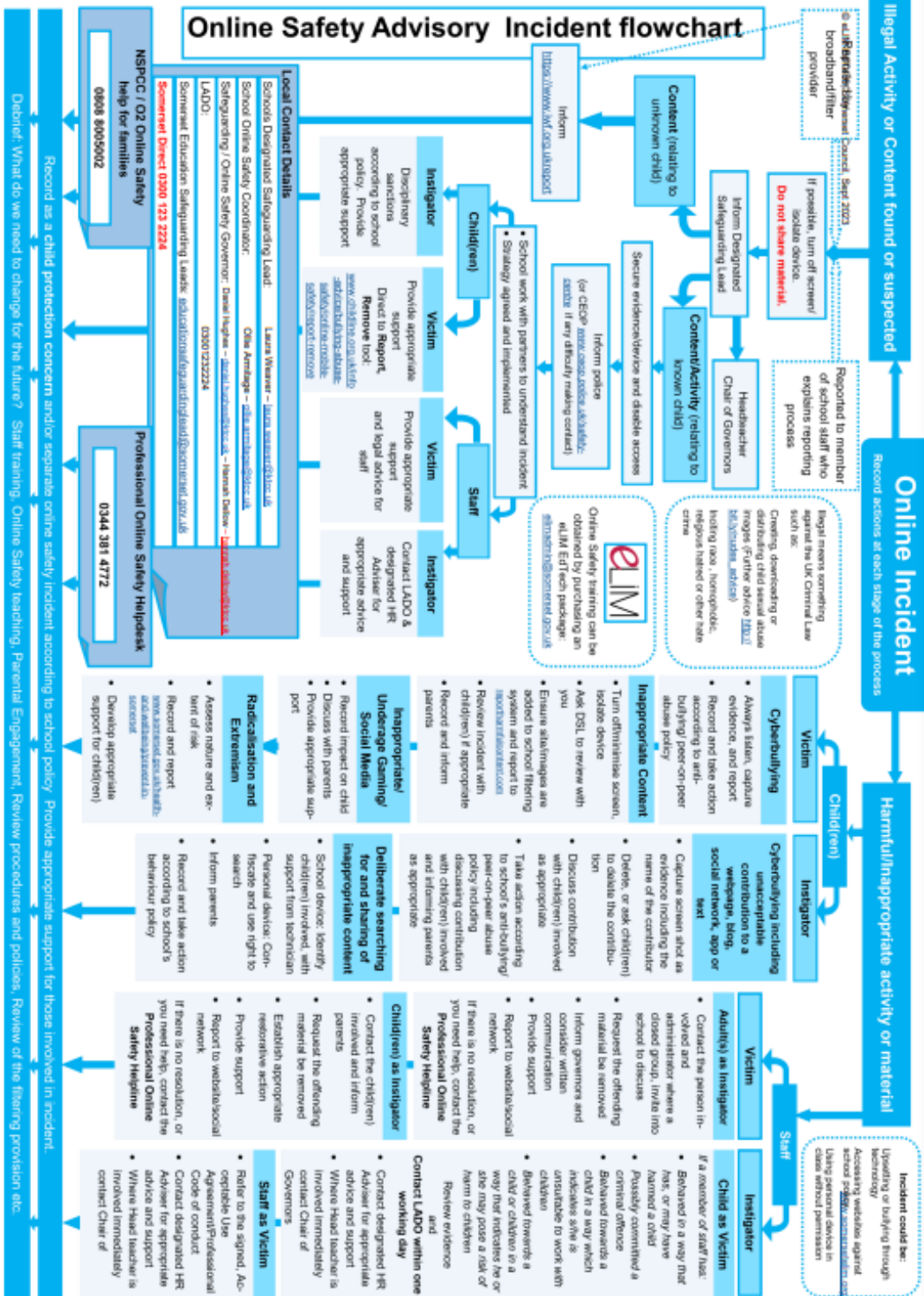
#### 6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority. The above Terms of Reference have been agreed.

Signed by (SLT): ..... Date:.....

Date for review: .....

Responding to incidents of misuse – flow chart



# Knights Templar Community Church School and Nursery



*"Be the best you can be with a zest for living, a thirst for learning and a spirit of kindness."*

Head Teacher: Mrs Laura Weaver, BA Hons QTS

*Record of reviewing devices/internet sites (responding to incidents of misuse)*

Group: .....

Date: .....

Reason for investigation: .....

.....  
.....

*Details of first reviewing person*

Name: .....

Position: .....

Signature: .....

*Details of second reviewing person*

Name: .....

Position: .....

Signature: .....

*Name and location of computer used for review (for web sites)*

.....  
.....

<i>Web site(s) address/device</i>	<i>Reason for concern</i>

<i>Conclusion and Action proposed or taken</i>	

A Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported	Signature
			What?	By Whom?	By	

*Training Needs Audit Log*

*Group:* .....

<i>Relevant training the last 12 months</i>	<i>Identified Training Need</i>	<i>To be met by</i>	<i>Cost</i>	<i>Review Date</i>

# Knights Templar Community Church School and Nursery



*“Be the best you can be with a zest for living, a thirst for learning and a spirit of kindness.”*

Head Teacher: Mrs Laura Weaver, BA Hons QTS

## *Technical Security Policy Template (including filtering, monitoring and passwords)*

*The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:*

- users can only access data to which they have right of access*
- access to personal data is securely controlled in line with the school's personal data policy*
- system logs are maintained and reviewed to monitor user activity*
- there is effective guidance and training for users*
- there are regular reviews and audits of the safety and security of school computer systems, including filtering and monitoring provision*

## *Responsibilities*

*The management of technical security is the responsibility of Governors and Senior Leaders, supported in this by the Designated Safeguarding Lead, Online Safety Coordinator and IT Service Provider- SWgFL.*

## *Policy statements*

*The school is responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:*

- school technical systems will be managed in ways that ensure that the school meets recommended technical requirements -these are outlined in our Local Authority technical guidance*
- cyber security is included in the school risk register.*
- there will be regular reviews and audits of the safety and security of school technical systems.*
- servers, wireless systems, and cabling must be 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 or in the cloud,*
- *appropriate security measures (including updates) are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data, including operating systems.*
- *the school's infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.*
- *responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff*
- *all users will have clearly defined access rights to school technical systems and accounts are deleted when the user leaves. Details of the access rights available to groups of users will be recorded by the network manager/technical staff/other person and will be reviewed, at least annually, by the online safety group.*
- *users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security*
- *The IT Service Provider, in partnership with Governors/SLT/DSL, regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.*
- *mobile device security and management procedures are in place*
- *an appropriate system is in place for users to report any actual/potential technical incident to the SLT/DSL/Online Safety Lead (OSL)/ (or other relevant person, as agreed)*
- *The Online Coordinator is 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 installations*
- *remote management tools are used by staff to control workstations and view users' activity.*
- *guest users are provided with appropriate access to school systems based on an identified risk profile.*
- *by default, users do not have administrator access to any school-owned device.*
- *unacceptable use 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 agreed policy is in place regarding the use of removable media by users on school devices*

- *personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

### **Password Security**

*A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform).*

### **Policy Statements:**

- *The password policy and procedures reflect NCSC and DfE advice/guidance.*
- *The use of passwords is reduced wherever possible, for example, using Multi-Factor Authentication (MFA) or (Single Sign On) SSO.*
- *Security measures are in place to reduce brute-force attacks and common passwords are blocked.*
- *School networks and system will be protected by secure passwords.*
- *Passwords are encrypted by the system to prevent theft.*
- *Staff Users are able to reset their password themselves..*
- *Passwords are immediately changed in the event of a suspected or confirmed compromise.*
- *No default passwords are in use. All passwords provided “out of the box” are changed to a unique password by the IT Service Provider.*
- *All accounts with access to sensitive or personal data are protected by Multi-Factor Authentication methods.*
- *A copy of administrator passwords is kept in a secure location.*
- *All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.*
- *Passwords must not be shared with anyone.*

### **Learner passwords:**

#### *Policy Statements*

- *For younger children and those with special educational needs, learner usernames and passwords can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.*

- Password complexity for these users are reduced (for example 6-character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.
- Learners are encouraged to set passwords with an increasing level of complexity. Passwords using 3 three random words and with a length of over 12 characters are considered good practice.
- Users will be required to change their password if it is compromised.
- Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

## **Filtering and Monitoring**

### **Introduction to Filtering**

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, as online content changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use.

Our filtering system is operational, up to date and applied to all:

- users, including guest accounts.
- school owned devices
- devices using the school broadband connection.

Our filtering system

- filter all internet feeds, including any backup connections.
- be age and ability appropriate for the users and be suitable for educational settings.
- handle multilingual web content, images, common misspellings and abbreviations.
- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them.
- provide alerts when any web content has been blocked.

Mobile and app content is often presented in a different way to web browser content. If your users access content in this way, you should get confirmation from your provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.

### **Introduction to Monitoring**

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

### Filtering and Monitoring Responsibilities

DfE Filtering Standards require that schools and colleges identify and assign roles and responsibilities to manage your filtering and monitoring systems, and include

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	Daniel Hughes
Senior Leadership	<p>Team Member Responsible for ensuring these standards are met and:</p> <ul style="list-style-type: none"> <li>• procuring filtering and monitoring systems</li> <li>• documenting decisions on what is blocked or allowed and why</li> <li>• reviewing the effectiveness of your provision</li> <li>• overseeing reports</li> </ul> <p>Ensure that all staff:</p> <ul style="list-style-type: none"> <li>• understand their role</li> <li>• are appropriately trained</li> <li>• follow policies, processes and procedures</li> <li>• act on reports and concerns</li> </ul>	Headteacher- Laura Weaver
Designated Safeguarding Lead	<p>Lead responsibility for safeguarding and online safety, which could include overseeing and acting on:</p> <ul style="list-style-type: none"> <li>• filtering and monitoring reports</li> <li>• safeguarding concerns</li> <li>• checks to filtering and monitoring systems</li> </ul>	<p>Laura Weaver- DSL</p> <p>Alex Walker- DDSL</p>
IT Service Provider	<p>Technical responsibility for:</p> <ul style="list-style-type: none"> <li>• maintaining filtering and monitoring systems</li> <li>• providing filtering and monitoring reports</li> </ul>	SWGfL

	<ul style="list-style-type: none"> <li>• completing actions following concerns or checks to systems</li> </ul>	
<p>All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:</p>	<ul style="list-style-type: none"> <li>• they witness or suspect unsuitable material has been accessed</li> <li>• they can access unsuitable material</li> <li>• they are teaching topics which could create unusual activity on the filtering logs</li> <li>• there is failure in the software or abuse of the system</li> <li>• there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks</li> <li>• they notice abbreviations or misspellings that allow access to restricted material</li> </ul>	All staff

### **Policy Statements**

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- There is a filtering and monitoring system in place that safeguards staff and learners by blocking harmful, illegal and inappropriate content.
- There is a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged.

- Roles and responsibilities for the management of filtering and monitoring systems have been defined and allocated.
- The filtering and monitoring provision is reviewed at least annually and checked regularly.
- There is a defined and agreed process for making changes to the filtering or monitoring system that involves a senior leader in the agreement of the change.
- Mobile devices that access the school's internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.

### **Changes to Filtering and Monitoring Systems**

To understand and evaluate the changing needs and potential risks of the school, the filtering and monitoring provision will be reviewed termly. The review will be conducted by members of the Online Safety Group. Additional checks to filtering and monitoring will be informed by the review process so that governors have assurance that systems are working effectively and meeting safeguarding obligations.

### **Reviewing the filtering and monitoring provision**

A review of filtering and monitoring will be carried out to identify the current provision, any gaps, and the specific needs of learners and staff.

The review will take account of:

- the risk profile of learners, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what the filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of learners
- teaching requirements, for example, the RHSE and PSHE curriculum
- the specific use of chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies are in place
- what checks are currently taking place and how resulting actions are handled

To make the filtering and monitoring provision effective, the review will inform:

- *related safeguarding or technology policies and procedures*
- *roles and responsibilities*
- *training of staff*
- *curriculum and learning opportunities*
- *procurement decisions*
- *how often and what is checked*
- *monitoring strategies*

*The review will be carried out as a minimum annually, or when:*

- *a safeguarding risk is identified*
- *there is a change in working practice, e.g. remote access or BYOD*
- *new technology is introduced*

#### *Checking the filtering and monitoring systems*

*Checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place will be based on the context, the risks highlighted in the filtering and monitoring review, and any other risk assessments. Checks will be undertaken from both a safeguarding and IT perspective.*

*When filtering and monitoring systems are checked this should include further checks to verify that the system setup has not changed or been deactivated. Checks are performed on a range of:*

- *school owned devices and services, including those used off site*
- *geographical areas across the site*
- *user groups, for example, teachers, pupils and guests*

*Logs of checks are kept so they can be reviewed. These are recorded:*

- *when the checks took place*
- *who did the check*
- *what was tested or checked*
- *resulting actions*

### **Training/Awareness:**

Governors, Senior Leaders and staff are made aware of the expectations of them:

- at induction
  - at whole-staff/governor training
  - through the awareness of policy requirements
  - through the acceptable use agreements
- in regular updates throughout the year

Those with specific responsibilities for filtering and monitoring will receive enhanced training to help them understand filtering and monitoring systems and their implementation and review.

Learners are made aware of the expectations of them:

- in lessons
- through the acceptable use agreements

Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter etc. (amend as relevant)

### **Audit/Monitoring/Reporting/Review:**

Governors/SLT/DSL/OSC will ensure that full records are kept of:

- Training provided
- User Ids and requests for password changes
- User logons
- Security incidents related to this policy
- Annual online safety reviews including filtering and monitoring
- Changes to the filtering system
- Checks on the filtering and monitoring systems

### **Further Guidance**

Schools in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering". Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges

in England to “ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness” and they “should be doing all that they reasonably can to limit children’s exposure to the above risks from the school’s or college’s IT system” however, schools will need to “be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.” Ofsted concluded as far back as 2010 that “Pupils in the schools that had ‘managed’ systems had better knowledge and understanding of how to stay safe than those in schools with ‘locked down’ systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves.”

To further support schools and colleges in England, the Department for Education published Digital and Technology standards.

The UK Safer Internet Centre has produced guidance on “[Appropriate Filtering and Monitoring](#)”  
SWGfL, on behalf of UK Safer Internet Centre and DfE, developed further [Filtering and Monitoring | SWGfL](#)  
information for schools and colleges, including a checklist alongside further support for Governors  
SWGfL provides a site for schools to test their filtering to ensure that illegal materials cannot be accessed: [SWGfL Test Filtering](#)

# Knights Templar Community Church School and Nursery



*“Be the best you can be with a zest for living, a thirst for learning and a spirit of kindness.”*

Head Teacher: Mrs Laura Weaver, BA Hons QTS

## ***Electronic devices - Searching, screening and confiscating.***

### *Introduction*

#### *Relevant legislation:*

- *Education Act 1996*
- *Education and Inspections Act 2006*
- *Education Act 2011 Part 2 (Discipline)*
- *The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012*
- *Health and Safety at Work etc. Act 1974*
- *Obscene Publications Act 1959*
- *Children Act 1989*
- *Human Rights Act 1998*
- *Computer Misuse Act 1990*

*This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.*

### ***Responsibilities***

*This policy has been written by Online Safety Coordinator and will be reviewed by Online Safety Group*

*The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data/files on those devices:*

- *DSL and Head teacher- Laura Weaver*
- *OSC- Ollie Armitage*
- *Key stage 2 lead- Kathy Larkins*
- *Key stage 1 lead- Alexandra Walker*
- *EYFS Lead- Gemma Cody-Boucher*

The Headteacher may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

#### **Training/Awareness**

Members of staff should be made aware of the school's policy on "Electronic devices – searching, confiscation and deletion":

- at induction
- at regular updating sessions on the school's online safety policy

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data/files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

#### **Screening Search**

This policy refers only to the searching for and of electronic devices and the deletion of data/files on those devices.

Year 4 Learners, in the Summer term, are allowed to bring mobile phones to school to be safely stored and only use them only within the rules laid down by the school.

If learners breach these rules:

The sanctions for breaking these rules can be found in the Online Safety policy.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent – Authorised staff may search with the learner's consent for any item
- Searching without consent – Authorised staff may only search without the learner's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for

*In carrying out the search:*

*The authorised member of staff must have reasonable grounds for suspecting that a learner is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.*

*The authorised member of staff should take reasonable steps to check the ownership of the mobile phone/personal electronic device before carrying out a search.*

*The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the learner being searched.*

*The authorised member of staff carrying out the search must be the same gender as the learner being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the learner being searched.*

*There is a limited exception to this rule: Authorised staff can carry out a search of a learner of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.*

***Extent of the search:***

*The person conducting the search may not require the learner to remove any clothing other than outer clothing. Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).*

*'Possessions' means any goods over which the learner has or appears to have control – this includes desks, lockers and bags.*

*A learner's possessions can only be searched in the presence of the learner and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.*

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

### *Electronic devices*

The DfE guidance – *Searching, Screening and Confiscation* received significant updates in July 2022 and now states:

- *Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.*
- *As with all prohibited items, staff should first consider the appropriate safeguarding response if they find images, data or files on an electronic device that they reasonably suspect are likely to put a person at risk*
- *Staff may examine any data or files on an electronic device they have confiscated as a result of a search if there is good reason to do so (defined earlier in the guidance as)*
  - *poses a risk to staff or pupils;*
  - *is prohibited, or identified in the school rules for which a search can be made or*
  - *is evidence in relation to an offence.*
- *If the member of staff conducting the search suspects they may find an indecent image of a child (sometimes known as nude or semi-nude images), the member of staff should never intentionally view the image, and must never copy, print, share, store or save such images. When an incident might involve an indecent image of a child and/or video, the member of staff should confiscate the device, avoid looking at the device and refer the incident to the designated safeguarding lead (or deputy) as the most appropriate person to advise on the school's response. Handling such reports or concerns can be especially complicated and schools should follow the principles as set out in *Keeping children safe in education*. The UK Council for Internet Safety also provides the following guidance to support school*

staff and designated safeguarding leads: Sharing nudes and semi-nudes: advice for education settings working with children and young people.

- If a member of staff finds any image, data or file that they suspect might constitute a specified offence, then they must be delivered to the police as soon as is reasonably practicable.
- In exceptional circumstances members of staff may dispose of the image or data if there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files, the member of staff must have regard to the following guidance issued by the Secretary of State
  - In determining whether there is a 'good reason' to examine the data or files, the member of staff should reasonably suspect that the data or file on the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.
  - In determining whether there is a 'good reason' to erase any data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable. If the data or files are not suspected to be evidence in relation to an offence, a member of staff may delete the data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves

#### **Care of Confiscated Devices**

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage/loss of such devices

#### **Audit/Monitoring/Reporting/Review**

The responsible person, Laura Weaver, will ensure that full records are kept of incidents involving the searching for and of electronic devices and the deletion of data/files.

These records will be reviewed by the Online Group at regular termly.

This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance and evidence gained from the records.

### *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.*

<b>CPD</b>	<i>Continuous Professional Development</i>
<b>FOSI</b>	<i>Family Online Safety Institute</i>
<b>ICO</b>	<i>Information Commissioners Office</i>
<b>ICT</b>	<i>Information and Communications Technology</i>
<b>INSET</b>	<i>In Service Education and Training</i>
<b>IP address</b>	<i>The label that identifies each computer to other computers using the IP (internet protocol)</i>
<b>ISP</b>	<i>Internet Service Provider</i>
<b>ISPA</b>	<i>Internet Service Providers' Association</i>
<b>IWF</b>	<i>Internet Watch Foundation</i>
<b>LA</b>	<i>Local Authority</i>
<b>LAN</b>	<i>Local Area Network</i>
<b>MIS</b>	<i>Management Information System</i>
<b>NEN</b>	<i>National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.</i>
<b>Ofcom</b>	<i>Office of Communications (Independent communications sector regulator)</i>
<b>SWGfL</b>	<i>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</i>
<b>TUK</b>	<i>Think U Know – educational online safety programmes for schools, young people and parents.</i>
<b>UKSIC</b>	<i>UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.</i>
<b>UKCIS</b>	<i>UK Council for Internet Safety</i>
<b>VLE</b>	<i>Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,</i>
<b>WAP</b>	<i>Wireless Application Protocol</i>

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