ST JOHN'S BEAUMONT

Online Safety Policy

This policy is applicable to the whole school community (including staff, learning, volunteers, boarding, Early Years Foundation Stage, parents and carers, visitors and 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 (where allowed).

Information Sharing Category	**All Staff**
Version	**2026-27v1**
Date Published	**June 2026**
Review Date	**June 2027**
Authorised by	**SLT**
Responsible Area	**Whole School**

Agreed by:

Headteacher	Deputy Head Pastoral	IT Manager
Mr Philip Barr	**Mr Jack Snell**	**Mr Lakhbir Branch**

Review Log	
LBr & JSn discussed Online Safety Policy Updates	8th June 2026

CONTENTS:

1. Introduction 3
2. Online Safety Policy 4
Scope of the online safety policy 4
Monitoring and Review of the Policy 5
Process for monitoring the impact of the online safety policy 5
3. Policy and Leadership 6
Roles and Resposibilities 6
Professional Standards 10
4. Policy 11
Online Safety Policy 11
Acceptable use 11
Reporting and Responding 15
Responding to Learner Actions 19
Responding to Staff Actions 20
The use of Artificial Intelligence (AI) systems in School 21
Teaching about Online Safety 23
Contribution of Learners 25
Educating Staff/Volunteers 25
Educating Governors 25
Educating Parents and Families 26
5. Online Safety Issues 26
Online Safety Issues 26
Child-on-Child Abuse 26
Harmful online challenges and online hoaxes 27
Radicalisation and the Use of Social Media to Encourage Extremism 28
Cyber-Bullying 28
Online Sexual Harassment 30
ICT-Based Sexual Abuse 31
Chat Room Grooming and Offline Abuse 32
6. Technology 32
Pupils' Use of IT Systems 32
How is the Content Filtered? 33
Protecting Personal Data 34
Assessing Risks 34

Mobile Electronic Devices....35
Social Media, including TikTok, SnapChat, Facebook, Xand Instagram....36
Communicating and educating parents/carers in online safety....36
Taking and Storing Images of Pupils Including Mobile Phones....37
Remote Learning....38
Cyber Security....38
7. Legal Status....39
Related documents....40
8. Appendix....41
A1 Learner Acceptable Use Agreement Template – for Year 6, 7 & 8....41
A2 Learner Acceptable Use Agreement for Years 3, 4 & 5....44
A3 Learner Acceptable Use Agreement (EYFS/KS1)....46
A4 Parent Acceptable Use Agreement....47
A5 Staff (and Volunteer) Acceptable Use Policy Agreement....48
A6 Record of reviewing devices/internet sites (responding to incidents of misuse)....51
A7 Responding to incidents of misuse – flow chart....52
A8 Serious Incident Reporting Log....1
A9 Training Needs Audit Log....2

1. INTRODUCTION

1.1 The purpose of this policy is to safeguard pupils, staff and all members of the school community at St John's Beaumont. It details the actions and behaviour required from pupils and members of staff in order to maintain a safe electronic environment and is

based on current best practice and statutory guidance. There is a whole school approach to keeping pupils safe online and online safety is to be promoted by all staff and members of the school community. All who work, volunteer, or supply services to our school have an equal responsibility to understand and implement this policy and its procedures both within and outside of normal school hours including activities away from school.

1.2 There are defined roles and responsibilities for online safety as part of the school's wider safeguarding strategy.

1.3 Online safety is a running and interrelated theme when devising and implementing our wider school policies and procedures, including our Child Protection & Safeguarding Policy.

1.4 The staff and pupil IT Acceptable Use Policies are central to the Online Safety Policy and should be consulted alongside this policy.

1.5 Online safety is part of the IT curriculum, staff training, and also through parental engagement.

1.6 The Online Safety Policy will be reviewed annually by the safeguarding team who will provide recommendations for updating the policy in the light of experience and changes in legislation or technologies.

1.7 The Pupil Parliament will be consulted regarding any changes to the IT Acceptable Use Policy for Pupils. All staff should read these policies in conjunction with the Online Safety Policy.

1.8 Online safety is an important part of the Prevent Strategy, as a large portion of cases of radicalisation happen online. Staff must be vigilant when dealing with such matters and ensure that they observe the procedure for reporting such concerns in line with that laid out in the Child Protection & Safeguarding Policy.

2. ONLINE SAFETY POLICY

SCOPE OF THE ONLINE SAFETY POLICY

2.1 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 and through normal communication channels (to be described).
- is published on the school website.

MONITORING AND REVIEW OF THE POLICY

2.2 This policy is subject to continuous monitoring, refinement and audit by the Headmaster and the Designated Safeguarding Lead (DSL) and Safeguarding Team. The Governing Council will undertake a full annual review of this policy and procedures, inclusive of its implementation and the efficiency with which the related duties have been discharged. This discussion will be formally documented in writing.

PROCESS FOR MONITORING THE IMPACT OF THE ONLINE SAFETY POLICY

2.3 The school will monitor the impact of the Online Safety Policy using:

- Logs of reported incidents
- Filtering and monitoring logs and checks
- Internal monitoring data for network activity
- Surveys of learners, parents and staff

2.4 All staff will be informed of the updated/reviewed policy and it is made available to them in either a hard copy or electronically.

2.5 The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by members of the senior leadership team, the designated safeguarding lead, and technical staff. It will also involve the responsible governor. The results of the review will be recorded and reported as relevant.

2.6 Evidence of filtering and monitoring reviews will be formally recorded and retained. Review records will include:

- the date of the review and testing activity;
- the devices, user groups and locations tested;
- the members of staff undertaking the review;

- any identified safeguarding concerns, vulnerabilities, filtering gaps or over-blocking issues;
- actions arising from the review, including agreed timescales and responsible staff;
- confirmation that identified issues have been resolved or otherwise escalated for further action.

2.7 Review records will be maintained by the DSL and IT Manager and made available to the Safeguarding Governor as part of the school's annual filtering and monitoring review process.

2.8 The DSL will maintain an operational understanding of the school's filtering and monitoring systems, associated reporting processes and escalation pathways.

2.9 Records of filtering and monitoring checks will be maintained and reviewed by the DSL, IT Manager and Safeguarding Governor. These records will include testing outcomes, identified concerns and remedial actions taken.

3. POLICY AND LEADERSHIP

ROLES AND RESPOSIBILITIES

3.1 The Headteacher/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 (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- The Headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, 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.
- Online searches undertaken as part of safer recruitment procedures are addressed within the school's Safer Recruitment Policy. The school recognises that online searches form part of the wider safeguarding culture and support the identification of information relevant to an applicant's suitability to work with children.
- 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 / Online Safety Lead.

- The Headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.
- The Deputy Head Pastoral (DSL) is the designated Senior Leadership Team member responsible for filtering and monitoring arrangements across the school.

3.2 Our nominated Online Safety Lead (OSL) is Jack Snell (DSL) who, along with the members of the safeguarding team, has responsibility for ensuring that online safety is considered an integral part of everyday safeguarding practice. The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Records of filtering and monitoring checks will be maintained and reviewed by the DSL, IT Manager and Safeguarding Governor. These records will include testing outcomes, identified concerns and remedial actions taken.
- 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 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/groups
- report regularly to Headteacher/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 DSL and DDSLs will be responsible for ensuring:

- agreed policies and procedures are to be implemented in practice.
- all updates, issues and concerns are to be communicated to all ICT users.
- the importance of online safety in relation to safeguarding is to be understood by all ICT users.
- the training, learning and development requirements of staff are to be monitored and additional training needs identified and provided for boarding specific training
- an appropriate level of access authorisation is given to ICT users.
- the curriculum addresses online safety.
- a safe ICT learning environment is to be promoted and maintained.

3.3 In collaboration with the on-site IT Manager, Lakhbir Branch, the Online Safety Officer and Designated Safeguarding Team have the responsibility of ensuring:

- Pupils know how to use the Internet and connected devices responsibly and that parents and teachers have the right measures in place to keep pupils safe from exploitation or radicalisation.
- Pupils are safe from terrorist and extremist material when accessing the Internet in school, including by establishing appropriate levels of filtering.
- Pupils use Information and Communications Technology (ICT) safely and securely and are aware of both external and child-on-child risks when using ICT, including cyberbullying and other forms of abuse.
- Pupils, staff, the Governing Council and volunteers will receive the appropriate Online Safety training, guidance, time and resources to effectively implement online safety policies and procedures.
- Clear and rigorous policies and procedures are to be applied to the use/non-use of personal ICT equipment by all individuals who affect or come into contact with the Pre-Prep, Middle School and Upper School and Boarding settings. Such policies and procedures are to include the personal use of work-related resources.
- The IT Acceptable Use Policy is to be implemented, monitored and reviewed regularly, and for ensuring all updates are to be shared with relevant individuals at the earliest opportunity.
- Monitoring procedures are to be transparent and updated as agreed in school policies. Allegations of misuse or known incidents are to be dealt with appropriately and promptly, in line with the Behaviour and Discipline Policy, Staff Behaviour Policy, Low Level Concerns Policy, and Child Protection and Safeguarding Policy and in liaison with other agencies, where applicable.
- Effective online safeguarding support systems are to be put in place, for example, filtering controls, secure networks and virus protection to ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- An appropriate level of authorisation is to be given to ICT users. Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned. In some instances, explicit individual authorisation must be obtained for specific activities when deemed appropriate, and any concerns and incidents are to be reported in a timely manner in line with agreed procedures.
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- A current record of all staff and Pupils who are granted access to school ICT system is maintained.

3.4 The Governing Council's responsibilities: provide pupils with a safe environment in which to learn and be safeguarded online. The Governing Council will do all that they reasonably

can to limit children's exposure to risks when using the school's IT system. As part of this process, the Governing Council has ensured the school has appropriate filters and monitoring systems in place which are reviewed regularly to monitor their effectiveness. They ensure that the senior leadership team and relevant staff have an awareness and understanding of the provisions in place, how to manage them effectively and know how to escalate concerns when identified.

Safeguarding Governor, Matthew Fogg, and at times, the Chair of Governors, Andrew Johnson will have:

- regular meetings with the Designated Safeguarding Lead.
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended).
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually in collaboration with the Safeguarding Team.
- reporting to relevant governors group/meeting.
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards.

3.5 Curriculum Leads: will work with the DSL and Safeguarding Team to develop a planned and coordinated approach to online safety education. This will be provided through:

- PSHE and RSE Programmes
- IT Curriculum
- Assemblies
- Pastoral Programmes (e.g. STEER Tracking)
- Visiting Speakers
- Wellbeing Surveys
- Relevant national initiatives and opportunities (e.g. Safer Internet Day, Mental Health Awareness Week, Anti-bullying Week)

3.6 All Staff: must be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of St John's Beaumont, and to deal with incidents of such as a priority. All staff are responsible for ensuring they are up to date with current Online Safety issues, and this online Safety Policy. Cyber-bullying incidents will be reported in accordance with school's Anti-Bullying Policy. All staff will ensure they understand and adhere to our Staff IT Acceptable Use Policy, which they must sign and return to Safeguarding Team. Teachers will ensure they are confident in delivering the school's IT/Computing and Online Safety curriculum as required, identifying risks and reporting concerns as they arise. Staff will immediately report any suspected misuse or problem to the Safeguarding Team for investigation/action in line with school safeguarding procedures.

3.7 All staff members undergo safeguarding induction training that explicitly outlines their precise day-to-day operational roles, workflows, and reporting pathways for verifying network filtering and monitoring integrity. Staff must know how to spot, escalate, and log instances where unexpected overrides or blocks occur, ensuring that technical barriers are actively matched by staff vigilance during lessons. Parents play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents 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 (the school will need to decide if they wish parents/carers to acknowledge these by signature).
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images etc. (see parent AUA in the appendix).
- parents' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents 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).
- they will read the pupils IT Acceptable Use Policy ensuring their child understands full their responsibility as part of this policy.

3.8 All Pupils: will ensure they understand and adhere to our Pupil IT Acceptable Use Policy, which they must sign and return to the Safeguarding Team. Pupils are reminded of their responsibilities regarding the use of the school's ICT systems and equipment, including their expected behaviour.

3.9 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.

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.

4. POLICY

ONLINE SAFETY POLICY

4.1 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 and through normal communication channels (to be described)
- is published on the school website.

ACCEPTABLE USE

4.2 Staff/Volunteers Use of IT Systems: Access to the Internet and e-mail is provided to support the curriculum, support school administration and for staff professional development only. All staff must read and confirm by signature that they have read the Staff IT Acceptable Use Policy before using any school ICT resource. In addition:

- All staff including the Governing Council will receive appropriate Online Safety training, which is updated regularly through staff inset. Online Safety issues are embedded in all aspects of the curriculum and other activities.
- Access to systems should be made by authorised passwords, which must not be made available to any other person.
- At all times staff must take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse, using personal data only on secure password protected computers and other devices.
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit. Student internet usage is also monitored through Impero which monitors blocked search terms and websites.
- Occasionally pupils may need to research educational material that may normally result in websites being blocked (e.g., racism). In this situation, staff may request to remove these sites form the filtered list for the period of study. Every request to do so should be auditable with clear reason for the need.
- The internet can be used to actively gather personal information about individuals which may lead to undesirable consequences (e.g., SPAM, fraud, harassment or identity theft). Because of this, staff are advised to only use the school approved web browsers and email systems which have appropriate security in place. Additionally, files should not be saved directly from the internet unless they can first be scanned for computer viruses, malware, spyware and other malicious programmes.
- Staff should not communicate with pupils through electronic methods such as social networking sites, blogging, chat rooms, texts or private email. Instead, only the school email system should be used for this purpose.
- Educational materials made by and for classes and uploaded to password-protected YouTube channels, i.e., videos of lessons, activities or fieldtrips, must be logged for record-keeping purposes. This provides an opportunity to share best practices and resources and enable better teaching and learning outcomes.
- In order to strengthen the schools' defences against future cyber incidents, the school will require multi-factor authentication (MFA) on all appropriate staff, governor and administrative accounts wherever technically possible.

4.3 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
- Communication with parents
- The IT/Computing, PSHE & RSE Curriculum

4.4 The following table illustrates what acceptable and unacceptable use of IT.

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:	Child sexual abuse imagery Child sexual abuse / exploitation / grooming Terrorism Encouraging or assisting suicide Offences relating to sexual images i.e., revenge and extreme pornography Incitement to and threats of violence Hate crime Public order offences - harassment and stalking Drug-related offences Weapons / firearms offences Fraud and financial crime including money laundering					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) Gaining unauthorised access to school networks, data and files, through the use of computers/devices Creating or propagating computer viruses or other harmful files Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) Disable/Impair/Disrupt network functionality through the use of computers/devices Using penetration testing equipment (without relevant permission)					X

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	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright and intellectual property (including through the use of AI services)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
User Actions	Staff Day Pupils Boarders	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Online Gaming		XX		X	
	Online Shopping/Commerce		XX		X	
	File Sharing			X	XX	
	Social Media			X	XX	
	Messaging/Chat		XX		X	
	Entertainment/Streaming (e.g. Netflix, Disney+)		XX		X	
	Use of video broadcasting (e.g. YouTube/Twitch, TikTok)				XXX	
	Mobile phones may be brought to school		XX		X	
	Use of mobile phones for learning			X (school devices)	XX	

	Use of mobile phones in social time at school		XX		X	
	Taking photos on mobile phones or cameras			X (school devices)	XX	
	Use of other personal devices (e.g. tablets, gaming devices, laptops)				XXX	
	Use of personal e-mail in school or on network WIFI		X		XX	
	Use of school e-mail for personal emails				XXX	

4.5 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 a nominated person – 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.

REPORTING AND RESPONDING

4.6 St John's Beaumont has clear reporting mechanisms in place, available for all users to report issues and concerns. For staff, any concerns regarding Online Safety should be made to the Online Safety Officer who will review the issue and take the appropriate action. For pupils, they are taught to raise any concerns to their class teacher who will then pass this on to the Online Safety officer. Complaints of a child protection nature must be dealt with in accordance with our Child Protection & Safeguarding Policy.

4.7 The Designated Safeguarding Lead provides advice and support to other members of staff on protecting pupils from the risk of online radicalisation. The school ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism.

4.8 The school ensures staff have the knowledge and confidence to identify pupils at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism.

4.9 Staff safeguard and promote the welfare of pupils and know where and how to refer pupils and young people for further help as appropriate by making referrals as necessary to Channel.

4.10 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:

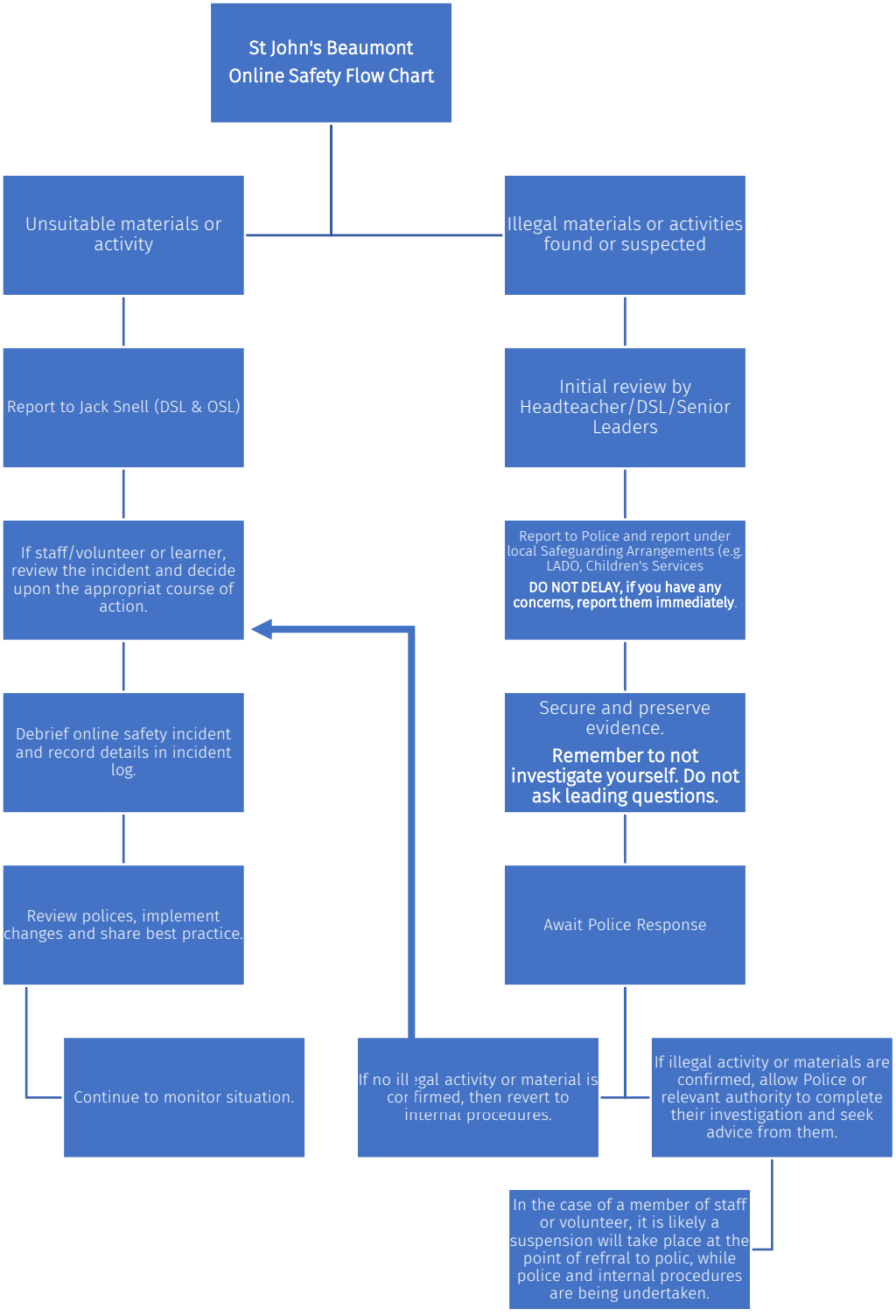
- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the low-level concerns, whistleblowing, complaints and managing allegations policies.
- all members of the school community 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 Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include:
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse or Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming o Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy

4.11 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.

4.12 Where there is no suspected illegal activity, devices may be checked using the following procedures:

- where the incident involves a member of staff, the Headteacher will contact the LADO and follow the advice given.
- for internal investigations, 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
    - further update to LADO
    - 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
- incidents should be logged using the template found in Appendix A5.
- 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 Safeguarding Team 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

4.13 Online Safety Incident Flow Chart



RESPONDING TO LEARNER ACTIONS

User Actions	Refer to class teacher/tutor	Refer to Head of School	Refer to DSL/Headteacher	Refer to police/children's services	Refer to IT Manager for technical support.	Inform parents	Remove device/network/internet access	issue warning	Further sanction, in line with behaviour & discipline 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
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
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature			X			X	X		X
Unauthorised downloading or uploading of files or use of file sharing.		X				X			X
Using proxy sites or other means to subvert the school's filtering system.			X		X	X			X
Accidentally accessing offensive or pornographic material and failing to report the incident.	X				X	X			
Deliberately accessing or trying to access offensive or pornographic material.			X		X	X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.					X	X			X
Unauthorised use of digital devices (including taking images)			X			X			X
Unauthorised use of online services			X			X			X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.			X			X			X

Continued infringements of the above, following previous warnings or sanctions.			X			X			X
Playing online games or watching inappropriate videos using a school device.	X	X							X

RESPONDING TO STAFF ACTIONS

User Actions	Refer to line manager	Refer to Headteacher	Refer to LADO	Refer to Police	Refer to IT Manager for technical support	Issue Warning	Suspension	Disciplinary Action	Further sanction, in line with behaviour & discipline 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
Actions which breach data protection or network / cyber-security rules.		X			X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material.		X	X	X			X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.		X			X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system.		X	X		X	X	X	X	X
Unauthorised downloading or uploading of files or file sharing.		X			X	X	X	X	X
Breaching copyright/ intellectual property or licensing regulations (including through the use of AI systems)		X			X	X			X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.		X		X	X	X	X	X	X

Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.		X	X	X		X	X	X	X
Using personal email/social networking/messaging to carry out digital communications with learners parents/carers.		X	X			X	X	X	X
Inappropriate personal use of digital technologies e.g. social media / email.		X	X			X	X	X	X
Careless use or personal data e.g. displaying, holding or transferring data in an insecure manner.		X			X	X	X	X	X
Actions which could compromise the staff member's professional standing.		X	X			X	X	X	X
Actions that could bring the school into disrepute or breach the integrity or ethos of the school.		X	X	X		X	X	X	X
Failing to report incidents whether caused by deliberate or accidental actions.		X	X			X	X	X	X
Continued infringements of the above, following previous warnings or sanctions.		X	X				X	X	X

THE USE OF ARTIFICIAL INTELLIGENCE (AI) SYSTEMS IN SCHOOL

4.14 The school recognises the potential safeguarding risks associated with emerging technologies, including AI-generated content (e.g. deepfakes, AI chatbots grooming children). Staff will continue to be trained to identify and escalate concerns as these technologies evolve.

4.15 We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

4.16 The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

4.17 The school acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools

to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.

4.18 We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR

4.19 We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.

4.20 We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.

4.21 As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.

4.22 Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.

4.23 Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. Any Generative AI platform, chatbot, or algorithmic tool procured or officially sanctioned for use within St John's Beaumont must strictly adhere to the DfE Generative AI: Product Safety Expectations guidance. The IT Department will verify that these systems effectively restrict algorithmic, dynamic, or unvetted output generation, ensuring that machine-learning interfaces do not bypass established school network filtering configurations. We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.

4.24 The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.

4.25 AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.

4.26 The school will audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.

4.27 We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.

4.28 The school will support parents and carers in their understanding of the use of AI in the school.

4.29 AI tools may be used to assist teachers in the assessment of learners' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI

4.30 Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.

4.31 We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.

4.32 Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

TEACHING ABOUT ONLINE SAFETY

4.33 The school's internet access is designed to enhance and extend education. Pupils will be taught what internet use is acceptable and what is not and given clear guidelines for internet use according to the Pupil IT Acceptable Use Policy.

4.34 Access levels reflect the curriculum requirements and age of pupils.

4.35 Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. The evaluation of on-line materials is a part of teaching/learning in every subject.

4.36 Staff should be vigilant in lessons where pupils use the internet by running Impero each time devices are used in lessons.

4.37 Staff will be provided with sufficient Online Safety training to protect pupils and themselves from online risks and to deal appropriately with Online Safety incidents when

they occur. Ongoing staff development training includes training on online safety, together with specific safeguarding issues including cyberbullying and radicalisation.

4.38 The frequency, level and focus of such training will depend on individual roles and requirements. Because new opportunities and challenges appear all the time, it is important that we focus our teaching on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app.

4.39 Online Safety is a focus in all areas of the curriculum and key online safety messages are reinforced regularly, teaching pupils about the risks of Internet use, how to protect themselves and their peers from potential risks, how to recognise suspicious, bullying or extremist behaviour and the consequences of negative online behaviour.

4.40 Access levels to ICT reflect the curriculum requirements and age of pupils. Staff should guide pupils to on-line activities that will support the learning outcomes planned for the pupils' age and maturity. This teaching is built into existing lessons alongside our wider whole-school approach.

4.41 Online safety lessons and digital safety messages must be explicitly differentiated for learners with Special Educational Needs and Disabilities (SEND). Teaching strategies must actively target specific cognitive or communication barriers, providing tailored guidance to help these students distinguish online reality from deceptive hoaxes, generated media, or targeted manipulation. Curriculum leads must ensure that SEND students are proactively supported so they do not mimic harmful viral trends or experience peer exclusion. Pupils will explicitly be taught the following topics through their lessons:

- What internet use is acceptable and what is not and given clear guidelines for internet use
- How to use a wide range of devices and learn about their advantages and disadvantages, in different applications
- How to evaluate what they see online
- How to recognise and respond to harmful online challenges and online hoaxes.
- How to recognise techniques used for persuasion
- Online behaviour
- How to identify online risks
- How and when to seek support
- How to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services)
- learners should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services

CONTRIBUTION OF LEARNERS

4.42 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.

EDUCATING STAFF/VOLUNTEERS

4.43 Online safety training opportunities will be available regularly to staff members (including the Governing Council) and content will include training on specific safeguarding issues, cyber bullying and radicalisation.

4.44 Staff will be provided with sufficient Online Safety training to protect pupils and themselves from online risks and to deal appropriately with Online Safety incidents when they occur.

4.45 The frequency, level and focus of such training will depend on individual roles and requirements.

4.46 Staff will undergo online safety training annually/when changes occur basis to ensure they are aware of current online safety issues and any changes to the provision of Online Safety, as well as current developments in social media and the internet as a whole.

4.47 Staff will be educated on which sites are deemed appropriate and inappropriate. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.

4.48 Any new staff members are required to undergo online safety training as part of their induction program, ensuring they fully understand this online safety policy, the social media policy and staff and pupil IT Acceptable Use Policy.

EDUCATING GOVERNORS

4.49 Governors should take part in online safety training/awareness sessions. For example, they may participate in school training / information sessions for staff/parents.

4.50 A higher level of training will be made available to (at least the Online Safety Governor). This will include cyber security (basic level) and 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 reviews.

EDUCATING PARENTS AND FAMILIES

4.51 Parents will be provided with a copy of the IT User Acceptance Policy, and parents will be asked to sign it, as well as pupils aged seven and older. St John's Beaumont recognises the crucial role that parents play in the protection of their children with regards to online safety. The school organises an annual awareness session for parents with regards to Online Safety which looks at emerging technologies and the latest ways to safeguard pupils from inappropriate content. The school will also provide parents and carers with information through newsletters, web site and the parent portals. Parents and guardians are always welcome to discuss their concerns on Online Safety with the school, who can direct them to the support of our Online Safety Officer if required. Parents and carers will be encouraged to support the school in promoting good Online Safety practice.

5. ONLINE SAFETY ISSUES

ONLINE SAFETY ISSUES

5.1 Breadth of Online Safety Issues: online safety issues can be classified into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, misinformation, disinformation, and conspiracy theories, racism, misogyny, antisemitism, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
- Commerce – risks such as online gambling, inappropriate advertising, phishing and or financial scams. These issues are to be managed by reducing availability, restricting access, promoting safe and responsible use.

CHILD-ON-CHILD ABUSE

5.2 St John's Beaumont recognises that child-on-child abuse can occur online and to this end we teach pupils how to spot early warning signs of potential abuse, and what to do if pupils are subject to sexual harassment online. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- access to illegal, harmful or inappropriate images
- cyber bullying
- access to, or loss of, personal information
- access to unsuitable online videos or games
- loss of personal images
- inappropriate communication with others
- illegal downloading of files
- exposure to explicit or harmful content, e.g., involving radicalisation
- plagiarism and copyright infringement
- sharing the personal information of others without the individual's consent or knowledge.

- All instances of online peer-to-peer abuse or harassment will be treated along a non-linear continuum of Harmful Sexual Behaviour (HSB). Response strategies will avoid rigid, automated punitive tracks; instead, the Safeguarding Team will apply a trauma-informed lens to determine if an online perpetrator is reacting to underlying offline trauma or extra-familial exploitation, triggering an Early Help Assessment alongside multi-agency contextual safeguarding protocols where appropriate.

HARMFUL ONLINE CHALLENGES AND ONLINE HOAXES

Please refer to the latest DfE Guidance: https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes

5.3 There has been a growing trend in the number of both challenges and hoaxes online as well as their popularity. As such, the school has put in a number of measures to safeguard our children. A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge. We teach pupils to recognise the signs that something may be untruthful online or that risks associated with any online challenges as well as who they can speak to if they have a concern. Where a child or member of staff reports an online hoax or challenge, we ensure that they are taken seriously, and acted upon appropriately, with the best interests of the child coming first. We ensure we provide opportunities to discuss this topic within Online Safety lessons, ensuring children and young people can ask questions and share concerns about what they experience online without being made to feel foolish or blamed.

5.4 A case-by-case assessment, establishing the scale and nature of the possible risk to our pupils will be carried out, and appropriate actions taken, which may include sharing information with parents and carers, our own young people as well as other local schools. Forward planning, together with case-by-case research, will allow for a calm and

measured response and avoid creating panic or confusion by spreading information which itself is untrue or would only draw pupils' attention to a potential risk.

5.5 The DSL will check the factual basis of any harmful online challenge or online hoax with a known, reliable and trustworthy source, such as the Professional Online Safety Helpline from the UK Safer Internet Centre. Where harmful online challenges or online hoaxes appear to be local (rather than large scale national ones) local safeguarding advice, such as from the local authority or local police force, may also be appropriate and helpful. Information that is shared with parents and carers will include encouraging them to focus on positive and empowering online behaviours with their children, such as critical thinking, how and where to report concerns about harmful content and how to block content and users.

RADICALISATION AND THE USE OF SOCIAL MEDIA TO ENCOURAGE EXTREMISM

5.6 The Internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs, sharing extreme ideological views or advocating the use of violence to solve problems. This has led to social media becoming a platform for:

- Intensifying and accelerating the radicalisation of young people
- Confirming extreme beliefs
- Accessing likeminded people where they are not able to do this off-line, creating an online community
- Normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

5.7 St John's Beaumont has a number of measures in place to help prevent the use of social media for this purpose:

- Web site filtering is in place on the school network to help prevent access to terrorist and extremist material and social networking sites such as TikTok, SnapChat, Facebook, Instagram, by pupils.
- Pupils, parents and staff are educated in safe use of social media and the risks posed by on-line activity, including from extremist and terrorist groups.

5.8 Further details on how social media is used to promote extremism and radicalisation can be found in guidance from the Department for Education 'How Social Media Is Used to Encourage Travel to Syria and Iraq: Briefing Note for Schools.'

CYBER-BULLYING

5.9 Cyber-Bullying is the use of ICT, particularly mobile electronic devices and the Internet, deliberately to upset someone else. Cyberbullying (along with all forms of bullying) will

not be tolerated and incidents of cyberbullying should be reported and will be dealt with in accordance with the school's Anti-Bullying Policy. Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline. If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the school's child protection procedures (see our Safeguarding & Child Protection Policy). Seven categories of cyber-bullying have been identified:

a) Text message bullying involves sending unwelcome texts that are threatening or cause discomfort;
b) Picture/video-clip bullying via mobile phone cameras is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks;
c) Phone call bullying via mobile phone uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified;
d) Email bullying uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them;
e) Chat room bullying and online grooming involve sending menacing or upsetting responses to pupils or young people when they are in a web-based chat room;
f) Bullying through instant messaging (IM) is an Internet-based form of bullying where pupils and young people are sent unpleasant messages through various messaging applications (for example, WhatsApp, Group Me, Skype, Facebook Messenger, Snapchat, Google Hangouts etc.) as they conduct real-time conversations online;
g) Bullying via websites and social networks (an example of this would be TikTok, SnapChat, Facebook, X, Instagram, etc.) includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyberbullying.

5.10 Pupils should remember the following:

- Always respect others – be careful what you say online and what images you send.
- Think before you send – whatever you send can be made public very quickly and could stay online forever.
- Don't retaliate or reply online.
- Save the evidence – learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to show what is happening and can be used by the school to investigate the matter.

- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving badly.
- Don't do nothing - if you see cyberbullying going on, support the victim and report the bullying.

ONLINE SEXUAL HARASSMENT

5.11 Sexual harassment creates an atmosphere that, if not challenged, can normalise inappropriate behaviours and provide an environment that may lead to sexual violence.

5.12 Online sexual harassment includes:

- non-consensual sharing of nude or semi-nude images and videos and sharing sexual images and videos (both often referred to as sexting); this includes AI-generated or digitally manipulated nude and semi-nude imagery, including deepfake content;
- inappropriate sexual comments on social media;
- exploitation;
- coercion and threats.

5.13 Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence.

5.14 All cases or allegations of sexual harassment, online or offline, is unacceptable and will dealt with under the school's Child Protection and Safeguarding Policy.

5.15 Additionally, we recognise that incidents of sexual violence and sexual harassment that occur online (either in isolation or in connection to offline incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and services and for things to move from platform to platform online. It also includes the potential for the impact of the incident to extend further than the school's local community (e.g., for images or content to be shared around neighbouring schools/colleges) and for a victim (or alleged perpetrator) to become marginalised and excluded by both online and offline communities. There is also the strong potential for repeat victimisation in the future if abusive content continues to exist somewhere online. Online concerns can be especially complicated.

5.16 The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772, and helpline@saferinternet.org.uk, providing expert advice and support for school staff with regard to online safety issues and when an allegation is received.

5.17 If the incident involves sexual images or videos that have been made and circulated online, we will support the victim to get the images removed through the Internet Watch Foundation (IWF). The IWF will make an assessment of whether the image is illegal in line with UK Law. If the image is assessed to be illegal, it will be removed and added to the IWF's Image Hash list.

5.18 Where an allegation or concern is raised regarding emerging or compulsive sexual thoughts or unsafe online behaviors among young people, the school will signpost and utilize the Lucy Faithfull Foundation's 'Shore Space' (shorespace.org.uk) resource. This platform provides a secure, confidential chat service designed to offer early preventative support for teenagers navigating problematic sexual behaviors or thoughts online.

ICT-BASED SEXUAL ABUSE

5.19 The impact on a child of ICT-based sexual abuse is similar to that for all sexually abused pupils. However, it has an additional dimension in that there is a visual record of the abuse. ICT-based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response are recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family. All adults (volunteers, staff) working with pupils, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the Internet or by mobile telephone;
- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images;
- An adult or older child may be viewing and downloading child sexual abuse images.

5.20 Pupils are reminded that sending nude or semi-nude images is strictly prohibited by the school and may constitute a criminal offence. Often referred to as 'sexting, the school will treat incidences of both sending and receiving these images as a safeguarding and/or child protection issue and pupils concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

5.21 There are no circumstances that will justify adults possessing indecent images of pupils. Adults who access and possess links to such websites will be viewed as a significant and potential threat to pupils. Accessing, making and storing indecent images of pupils is illegal. This will lead to criminal investigation and the individual being barred from working with pupils, if proven. Adults should not use equipment belonging to the school to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with pupils. Adults should ensure that pupils are not exposed to any inappropriate images or web links. Where indecent images of pupils or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate

the matter or evaluate the material themselves, as this may lead to evidence being contaminated, which in itself can lead to a criminal prosecution.

CHAT ROOM GROOMING AND OFFLINE ABUSE

5.22 Staff need to be continually alert to any suspicious activity involving computers and the Internet. Grooming of pupils online is a faster process than usual grooming, and totally anonymous. The abuser develops a 'special' relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child.

6. TECHNOLOGY

PUPILS' USE OF IT SYSTEMS

6.1 All pupils must agree to the Pupil IT Acceptable Use Policy before accessing the school systems. Pupils at St John's Beaumont will be given supervised access to computing facilities and will be provided with access to filtered Internet and other services operating at the school (Pupil internet usage is monitored through Impero which monitors blocked search terms and websites.).

6.2 The promotion of online safety within ICT activities is to be considered essential for meeting the learning and development needs of pupils and young people. The school will ensure that the use of internet-derived materials by staff and pupils complies with copyright law.

6.3 The school will help pupils to understand the risks posed by adults or young people, who use the internet and social media to bully, groom, abuse or radicalise other people, especially pupils, young people and vulnerable adults.

6.4 Internet safety is integral to the school's ICT curriculum and is also be embedded in our Personal, Social, Health and Economic Education (PSHE) and Spiritual, Moral, Social and Cultural (SMSC) Development. The latest resources promoted by the DfE can be found at:

- Education for a connected world
- The UK Safer Internet Centre (www.saferinternet.org.uk)
- CEOP's CEOP Education website (**https://www.ceopeducation.co.uk/**)
- Teaching Online Safety in School https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- Google Legends (KS2) (https://beinternetlegends.withgoogle.com/en_uk)

HOW IS THE CONTENT FILTERED?

6.5 Having Internet access enables students to explore thousands of global libraries, databases and bulletin boards. They are also able to exchange messages with other learners and teachers throughout the world. All unsuitable websites will be filtered and automatically blocked by our security systems (Sophos Web & Firewall / Impero) and will not be made accessible to students. In addition, students' usage of our network will be monitored continuously and repeated attempts to access unsuitable sites will alert our IT Department and DSL Team. The IT Department will tailor the filtering to suit the individual needs of subjects and the school generally appropriate to the age of students. Although this filtering uses the latest security technology, parents/guardians will wish to be aware that some students may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive to some people.

6.6 However, at St John's, we believe that the benefits to students having access to the Internet in the form of information, resources and opportunities for collaboration exceed any disadvantages. However, as with any other area, parents and guardians of minors along with St John's share the responsibility for setting and conveying the standards that students should follow when accessing and using the media information sources at school and/or at home. During school time, teachers will guide students towards appropriate material on the Internet. Outside school, families bear the same responsibility for guidance as they exercise with other information, sources such as television, telephones, films and radio.

6.7 Steps for managing filtering are:

- The school will work in partnership with parents/guardians, the Local Authority (LA) and Department for Education (DfE) to ensure systems to protect students are reviewed and improved.
- If staff or students come across unsuitable on-line materials, they must report it to the ICT Coordinator immediately.
- The school will take every step to ensure that appropriate filtering systems are in place to protect students from unsuitable material and the methods used will be reviewed regularly.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (https://www.iwf.org.uk).
- There are regular checks of the effectiveness of the filtering systems. Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The DSL and Governor are involved in the process and aware of the findings.
- Devices that are provided by the school have school-based filtering applied irrespective of their location. To ensure compliance with national digital infrastructure guidelines, the IT Manager and the Designated Safeguarding Lead (DSL) will jointly

utilise the Department for Education's statutory 'Plan technology for your school' service at least annually. This service will be used to self-assess the school's technical estate against active filtering and monitoring standards, generating baseline compliance reports and infrastructure optimisation recommendations to be presented directly to the Governing Council.

PROTECTING PERSONAL DATA

6.8 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the UK General Data Protection Regulations (UK GDPR). The school recognises that if required, data may need to be obtained by relevant parties such as the Police. Pupils are encouraged to keep their personal data private as part of our Online Safety lessons and IT curriculum, including areas such as password protection and knowledge about apps and unsecured networks/apps etc. The school will act responsible for ensuring we have an appropriate level of security protection procedures in place, in order to safeguard systems, staff and learners and we review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

6.9 Access to systems, applications and data will be provided on a least-privilege basis, ensuring that users are granted only the permissions necessary to perform their role. Access rights will be reviewed periodically and amended promptly when responsibilities change or employment ends.

ASSESSING RISKS

6.10 The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

6.11 Emerging technologies, such as mobile phones with Internet access (smartphones) are not governed by the school's infrastructure and bypass any and all security and filtering measures that are or could be deployed.

6.12 The school carries out an annual audit of our Online Safety provision in October to establish if the Online Safety Policy is sufficiently robust and that the implementation of the Online Safety Policy is appropriate and effective.

6.13 Methods to identify, assess and minimise risks will be reviewed regularly.

6.14 The Heads of School/Boarding will review and examine emerging technologies for educational benefit and a risk assessment will be carried out before use in school is allowed.

6.15 Any person not directly employed by the school will not be provided with access to any of the school systems with the exception of filtered Wi-Fi access.

6.16 The school takes measures to ensure appropriate IT filters monitoring systems are in place to safeguard pupils from potentially harmful and inappropriate material on-line without unreasonable "over-blocking"

6.17 The school recognises that pupils may choose to circumvent certain safety precautions by using devices over 3G, 4G and 5G. To help provide a safe environment for all pupils, we will supplement the systems filtering with behaviour management and additional staff/student training.

MOBILE ELECTRONIC DEVICES

6.18 Day School:

- Mobile phones are not permitted in the day school for pupils, or during regular school activities e.g. during home or away sports fixtures.
- If a device is brought to school, St John's Beaumont is not responsible for any devices lost by pupils.
- Recordings or live streaming made using mobile electronic devices (e.g. photograph / film / audio recording) is prohibited. The discovery of any uploads to social media platforms will result in serious sanctions being applied
- School devices may be used by teachers where there are children present, but any images captured must be erased from the device if a teacher leaves the school site with this device, unless this is for the purposes of an educational school trip.
- Pupils' mobile phones will be confiscated if found and returned only at the end of the school day.

6.19 Staff Personal Devices:

- Staff must not use personal mobile phones in the presence of pupils.
- Staff must not use personal mobile phones to take photographs, film or record pupils in any way.

6.20 EYFS Setting

- No personal mobile phones are to be used in the Early Years setting during the teaching day.
- All members of staff working in EYFS will not use or carry personal mobile phones while working.
- Staff may use their phones during break and lunchtimes in the staffroom only. Designated school devices may be used to take photos and record information of the children's learning.

6.21 Boarding

- Mobile telephones and laptops are permitted in both boarding houses on Tuesday and Thursday during 7 – 7:25pm for Years 3 to 7 pupils and 8:15 – 8:45pm for the year 8 pupils.
- Recordings or live streaming made using mobile electronic devices (e.g. photograph / film / audio recording) is prohibited. The discovery of any uploads to social media platforms will result in serious sanctions being applied.
- All electronic devices are welcome to be joined to the school network, school devices must be connected at all times to ensure proper filtering, and monitoring is taking place.

6.22 School trips

- The trip leader has discretion to allow the use of mobile phones during longer overnight school trips to allow for some contact with parents / carers.
- Teachers will be responsible for storing mobile phones and devices when not in use.
- As above, recordings or live streaming made using mobile electronic devices (e.g. photograph / film / audio recording) is prohibited during times when pupils are allowed access to their phones.

SOCIAL MEDIA, INCLUDING TIKTOK, SNAPCHAT, FACEBOOK, X AND INSTAGRAM

6.23 TikTok, SnapChat, Facebook, X, Instagram and other forms of social media are becoming an increasingly important part of our daily lives. Social media is very likely to play a central role in the fall out from any incident or alleged incident. There is the potential for contact between victim and alleged perpetrator and a very high likelihood that friends from either side could well harass the victim or alleged perpetrator online.

6.24 Staff are not permitted to access their personal social media accounts using school equipment at any time, unless granted prior permission by the Head Teacher for reasons of work. Staff and pupils are provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others. Staff and pupils, are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever. Staff and pupils are aware that their online behaviour should at all times be compatible with UK law.

COMMUNICATING AND EDUCATING PARENTS/CARERS IN ONLINE SAFETY

6.25 It is essential for parents/carers to be fully involved with promoting Online Safety both in and outside of school and to be aware of their responsibilities. The school regularly consult and discuss Online Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks. Parents will be provided with a copy of the Pupil IT Acceptable Use Policy, and parents of pupils from the Early Years to Year 3 will be asked to sign it on their child's behalf.

6.26 St John's Beaumont recognises the crucial role that parents play in the protection of their children with regards to Online Safety. The school organises annually awareness sessions for parents with regards to Online Safety, which look at emerging technologies and the latest ways to safeguard children from inappropriate content. The school will also provide parents and carers with information through newsletters, website; Parents/Carers sessions. Parents and carers are always welcome to discuss their concerns on Online Safety with the school. Parents and carers are encouraged to support the school in promoting good Online Safety practice.

- Parents/carers are required to decide whether they consent to images of their child being taken and used in the public domain (e.g., on school website).
- Parents/carers are expected to sign an agreement containing the following statement or similar:

  We will support the school approach to online safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community or bring the school's name into disrepute.

6.27 The school disseminates information to parents relating to Online Safety where appropriate in the form of; posters and school website

TAKING AND STORING IMAGES OF PUPILS INCLUDING MOBILE PHONES

6.28 St John's Beaumont provides an environment in which pupils, parents and staff are safe from images being recorded and inappropriately used. Upon their initial visit, parents, volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises in the presence of pupils, or to take photographs of pupils apart from circumstances as outlined in this policy. This prevents staff from being distracted from their work with pupils and ensures the safeguarding of pupils from inappropriate use of mobile phone cameras and other digital recording equipment. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images of themselves and others especially on social networking sites.
- Photographs published onto any website will comply with good practice guidance on the use of such images. Care will be taken to ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Their full names will not be used anywhere on the website, particularly in association with photographs.

6.29 The word 'camera' in this document refers to any device that may be used to take and store a digital image e.g., mobile phone, tablet, laptop etc.

REMOTE LEARNING

6.30 Where there are periods in which the school is forced to close yet continue to provide education (such as during significant rising respiratory infection rates, such as the Covid19 pandemic) it is important that St John's Beaumont supports staff, pupils and parents to access learning safely, especially considering the safety of our vulnerable pupils. Staff and volunteers are aware that this difficult time potentially puts all children at greater risk and the school recognises the importance of all staff who interact with children, including online, continuing to look out for signs a child may be at risk. Staff and volunteers will continue to be alert to any signs of abuse, or effects on learners' mental health that are also safeguarding concerns and will act on concerns immediately. Any such concerns should be dealt with as per the Child Protection & Safeguarding Policy and where appropriate referrals should still be made to children's social care and as required, the police.

6.31 Online teaching should follow the same principles as set out in the school's Staff Behaviour Policy and Behaviour and Discipline Policy.

6.32 The school will ensure any use of online learning tools and systems is in line with privacy and data protection/UK GDPR requirements.

6.33 The school will put additional measures in place to support parents and pupils who are learning from home. This will include specific guidance on which programmes the school is expecting pupils to use and how to access these alongside how pupils and parents can report any concerns that they may have. Guidance will also be issued on which staff members pupils will have contact with and how this will happen, including how to conduct virtual lessons (including video calls).

CYBER SECURITY

6.34 The DfE Cyber security standards for schools and colleges explains: "Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes
- a significant data breach
- significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
- financial loss

- reputational damage".

6.35 The school will conduct a cyber risk assessment annually and review each term

6.36 Staff and Governors receive training on the common cyber security threats and incidents that schools experience

6.37 The school's education programmes include cyber awareness for learners

6.38 There are processes in place for the reporting of cyber incidents.

6.39 The school will maintain a robust patch management process to ensure that operating systems, applications, devices, network infrastructure and security appliances are updated in a timely manner to reduce cyber security vulnerabilities.

6.40 The school will maintain secure backup and disaster recovery arrangements, including regular testing of restoration procedures to ensure critical systems and data can be recovered in the event of cyber incidents, system failures or data loss.

7. LEGAL STATUS

This policy has regard to the following guidance:

- Part 3, paragraphs 7 (a) and (b) of the Education (Independent School Standards) (England) Regulations 2014, and amendments to these.
- Keeping Children Safe in Education (KCSIE) Information for all schools and colleges (DfE, 2026)
- Disqualification under the Childcare Act 2006 Childcare (Disqualification) and Childcare (Early Years Provision Free of Charge) (Extended Entitlement) (Amendment) Regulations 2018.
- Working Together to Safeguard Children (WT) (2023)
- Prevent duty guidance: England and Wales (2023)
- The use of social media for on-line radicalisation (2015)
- How Social Media Is Used To Encourage Travel To Syria And Iraq: Briefing Note For Schools (DfE 2015)
- Cyberbullying: Advice for Heads and School staff (DfE 2014)
- Advice for parents and carers on cyberbullying (DfE 2014)
- Preventing and Tackling Bullying: Advice for school leaders and governors and the relevant aspects of Safe to Learn, embedding anti-bullying work in schools (DfE 2014)
- The DfE Don't Suffer in Silence booklet
- The Data Protection Act (2018)
- UK GDPR and Child Exploitation and Online Protection Command (CEOP).
- Teaching Online Safety in School (DfE, 2019)
- Education for a connected world (2020)

- Harmful Online challenges and online hoaxes (2021)
- NCSC Cyber Security Standards (2022)
- Filtering and Monitoring Standards (DfE)
- Cyber Security Standards (DfE)

RELATED DOCUMENTS

- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Behaviour and Discipline Policy
- PSHE & RSE Policy
- Safer Recruitment Policy

8. APPENDIX

A1 LEARNER ACCEPTABLE USE AGREEMENT TEMPLATE – FOR YEAR 6, 7 & 8

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the schools will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I will not arrange to meet people off-line that I have communicated with on-line. I will share any such requests with a parent or teacher.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school's systems and devices are intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school's systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

Following the St John's Beaumont Pupil Code of Conduct, I will:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I understand that Mobile phones and other personal devices are not permitted in the day school for pupils, or during regular school activities e.g. during home or away sports fixtures.
- I understand that, for school trips, the trip leader has discretion to allow the use of mobile phones during longer overnight school trips to allow for some contact with parents only.
- I understand that mobile telephones and personal devices are permitted in boarding houses on Tuesday and Thursday evening, and the weekend during set times.
- I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download, or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software; however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to school sanctions. This could include loss of access to the school network/internet, sanctions according to the Behaviour & Discipline Policy, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school devices and systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school's systems and devices (both in and out of school).
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices, personal devices.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, virtual learning platforms, websites with school log-ins etc.

Name of Learner: .....

Group/Class: .....

Signed: .....

Date: .....

Parent Countersignature: .....

A2 LEARNER ACCEPTABLE USE AGREEMENT FOR YEARS 3, 4 & 5

School Policy

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity, and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly.
- I will only visit internet sites that adults have told me are safe to visit.
- I will keep my username and password safe and secure and not share it with anyone else.
- I will be aware of "stranger danger" when I am online.
- I will not share personal information about myself or others when online.
- I will not arrange to meet people off-line that I have communicated with on-line. I will share any such requests with a parent or teacher.
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

Following the St John's Beaumont Pupil Code of Conduct, I will:

- When online, I will treat others as I wish to be treated.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others, and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I understand that Mobile phones and other personal devices are not permitted in the day school for pupils, or during regular school activities e.g. during home or away sports fixtures.
- I understand that, for school trips, the trip leader has discretion to allow the use of mobile phones during longer overnight school trips to allow for some contact with parents only.
- I understand that mobile telephones and personal devices are permitted in boarding houses on Tuesday and Thursday evening, and the weekend during set times.
- I will not use social media sites.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to school sanctions. This could include loss of access to the school network/internet, sanctions according to the Behaviour & Discipline Policy, contact with parents and in the event of illegal activities involvement of the police.

Learner Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school devices and systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school's systems and devices (both in and out of school).
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices, personal devices.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, virtual learning platforms, websites with school log-ins etc.

Name of Learner: .....

Group/Class: .....

Signed: .....

Date: .....

Parent Countersignature: .....

A3 LEARNER ACCEPTABLE USE AGREEMENT (EYFS/KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets.
- I will only use activities that a teacher has told or allowed me to use.
- I will take care of computers/tablets and other equipment.
- I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher if I see something that upsets me on the screen.
- I know that if I break the rules, I might not be allowed to use a computer/tablet.

Learner Acceptable Use Agreement Form

Name of Learner: .....

Group/Class: .....

Signed: .....

Date: .....

Parent Countersignature: .....

A4 PARENT ACCEPTABLE USE AGREEMENT

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that learners have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the learner acceptable use agreement is attached to this permission form, so that parents will be aware of the school expectations of the young people in their care. Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission form

As parent of the below learners, I give permission for my child to have access to digital technologies at school.

I know that my child has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

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

I understand that my child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

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

Name of Parent: .....

Name of Learner: .....

Signed: .....

Date: .....

A5 STAFF (AND VOLUNTEER) ACCEPTABLE USE POLICY AGREEMENT

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....

Signed: .....

Date: .....

A6 RECORD OF REVIEWING DEVICES/INTERNET SITES (RESPONDING TO INCIDENTS OF MISUSE)

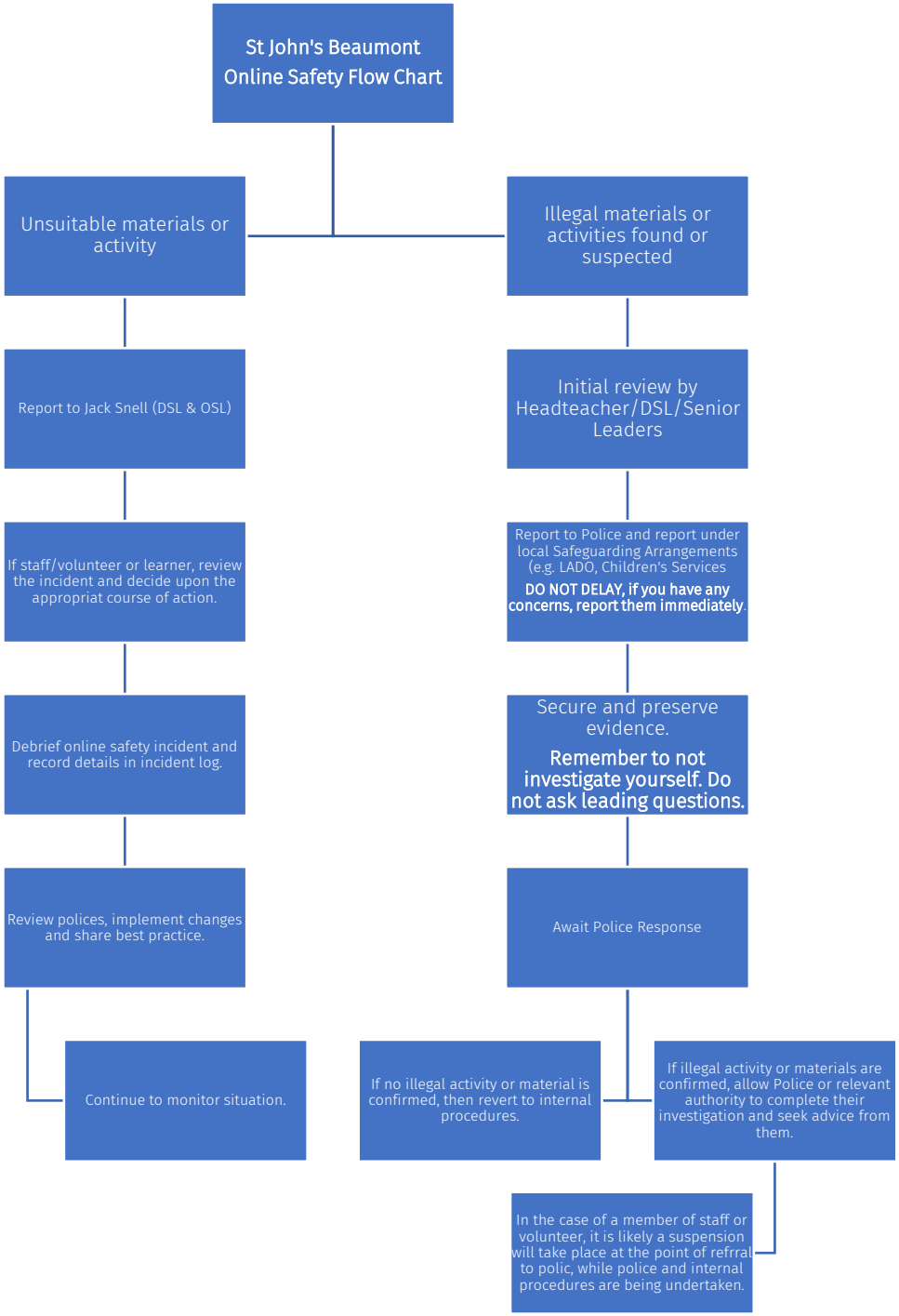
When recording Impero captures or incidents misuse, the screenshot of the capture should be uploaded to CPOMS under the pupil name. The screen shot will detail the reason for capture, as well as the date of incident. The CPOMS log should include:

- Reason for concern
- Conclusion and action proposed or taken

Alternatively, the below form can be used, scanned and uploaded to CPOMS.

Date:	
Reason for investigating:	
Details of person investigating:	
Details of person reviewing investigation:	
Pupil name:	
Time of incident:	
Location of incident:	
Website/device use:	
Reason for concern:	
Conclusion and action proposed or taken:	

A7 RESPONDING TO INCIDENTS OF MISUSE – FLOW CHART



ST JOHN'S BEAUMONT

A8 SERIOUS INCIDENT REPORTING LOG

Date	Time	Incident	Action Taken		Incident reported by	Signature
			What?	By whom?		

A9 TRAINING NEEDS AUDIT LOG

Relevant Training in Last 12 months	Identified Training Need	To be met by	Cost	Review date