Online Safety Policy

Date: March 2025

Approved by Advisory Board: March 2025

Review date: March 2026

Linked to policies:

Safeguarding including Child Protection

Signed: S. Day

Registered address: All Saints School (Lessingham) Limited. Company no: 10323174
Rookery Farm, Reynolds Lane, Potter Heigham, Great Yarmouth NR29 5LY

Version Control

Version	Date of review/change(s)	Page and paragraphs affected	Summary of update
New policy	March 2024		
V2	March 2025	P35	Paragraph added re. AI
	June 2025	P60	Appendix one added: Disclaimer statement re. mobile devices in school

Contents

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of All Saints School to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community (including staff, learners, advisors, volunteers, parents and carers, visitors,) who have access to and are users of 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).

All Saints School will deal with such incidents within the remit of this policy and the associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that takes place out of school.

Policy Development. Monitoring and review

This Online Safety Policy has been developed by the *Online Safety Group* made up of:

- Headteacher /Designated Safeguarding Lead (DSL)
- IT Manager who is also the Online Safety Lead (OSL)
- Staff – including teachers/support staff
- Advisor
- Parents and carers

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

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

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

Policy and Leadership

Responsibilities

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

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, through the day-to-day responsibility for online safety, as defined in Keeping Children Safe in Education.
- The Headteacher and school support manager are 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 is responsible for ensuring that the Designated Safeguarding Leads, IT manager /IT technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Headteacher 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 will receive regular monitoring reports from the Online Safety Lead.
- The Headteacher will work with the responsible advisor, the Designated Safeguarding Leads (DSL's) and IT Manager in all aspects of filtering and monitoring.

Directors and Advisors

Directors and advisors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy

This review will be carried out by the named advisor who will take on the role of Online Safety advisor to include:

- **regular meetings with the Designated Safeguarding Lead and IT Manager**
- **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.** (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible advisor) - in-line with the DfE Filtering and Monitoring Standards
- **reporting to advisory board**
- receiving (at least) basic cyber-security training to enable them to check that the school meets the DfE Cyber-Security Standards
- *acting as a member of the school Online Safety Group*

The advisory board will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safeguarding Lead (DSL) (the Headteacher)

will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety advisor to discuss current issues, review incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend advisory board meetings
- report regularly to the Directors

- be responsible for receiving reports of online safety incidents and handling them.
- decide 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 I.T. Manager who is the Online Safety lead (OSL)

will:

- lead the Online Safety Group
- be aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
- ensure the school technical infrastructure is secure and is not open to misuse or malicious attack
- enable the school to meet (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges
- ensure there is clear, safe, and managed control of user access to networks and devices
- keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- ensure the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to DSL for investigation and action
- ensure the filtering process is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- ensure monitoring systems are implemented and regularly updated as agreed in school policies
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL),
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/advisors/parents/carers/learners
- liaise with staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

*IT manager is supported by IT providers (Net Central, Phoenix, C learning)

Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme e.g. ProjectEVOLVE .

This will be provided through:

- a discrete programme
- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and Support Staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff Acceptable Use Agreement (AUA)
- they immediately report any suspected misuse or problem to the Headteacher or IT Manager (OSL) for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- learners understand and follow the Online Safety Policy and Acceptable Use Agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned, *learners are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Learners

- are responsible for using the school digital technology systems in accordance with the Learners' Acceptable Use Agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and Carers

The school will take every opportunity to help parents and carers understand these issues through:

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

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

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

Online Safety Group

The Online Safety Group has the following members

- Headteacher /Designated Safeguarding Lead
- IT Manager who is also the Online Safety Lead
- advisor
- school secretary
- teacher and / or support staff member
- learners
- parents/carers

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

- the production/review/monitoring of the school Online Safety Policy
- mapping and reviewing the online safety education provision – ensuring relevance, breadth, progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

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

Professional Standards

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

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 safeguarding briefings
- is published on the school website.

Acceptable use

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

Acceptable use agreements

The Online Safety Policy and Acceptable Use Agreement define acceptable use of digital technologies at the school. The Acceptable Use Agreement will be communicated/re-enforced through:

- student planner
- staff induction and handbook
- communication with parents/carers
- discreet education sessions as part of the curriculum
- school website
- peer support.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering					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	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				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes:	Staff and Other Adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/aware
Online gaming	X				X			
Online shopping/commerce				X	X			
File sharing		X					X	
Social media				X	X			
Messaging/Chat			X				X	
Entertainment streaming e.g. Netflix, Disney+			X		X			
Use of video broadcasting, e.g. YouTube, Twitch, Tiktok			X	X				X
Mobile phones may be brought into school		X				X		
Use of mobile phones for learning at school	X				X			
Use of mobile phones in social time at school			X		X			
Taking photos on mobile phones/cameras		X					X	
Use of other personal devices, e.g. tablets, gaming devices			X			X		
Use of personal e-mail in school, or on school network/wifi		X			X			
Use of school e-mail for personal emails	X				X			

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

- **when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.**
- **any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content.** *Personal e-mail addresses, text messaging or social media must not be used for these communications.*

- **staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community**
- **users should immediately report to the Headteacher in the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- *relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.*

Reporting and responding

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

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the Whistleblowing and Complaints 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, IT Manager 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), the incident must be escalated through the agreed school safeguarding procedures, this may include
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy

- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Advisory Board
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - the procedure should be conducted 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). The same device should be used for the duration of the procedure.

- the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - internal response or discipline procedures
    - involvement by local authority
    - police involvement and/or action

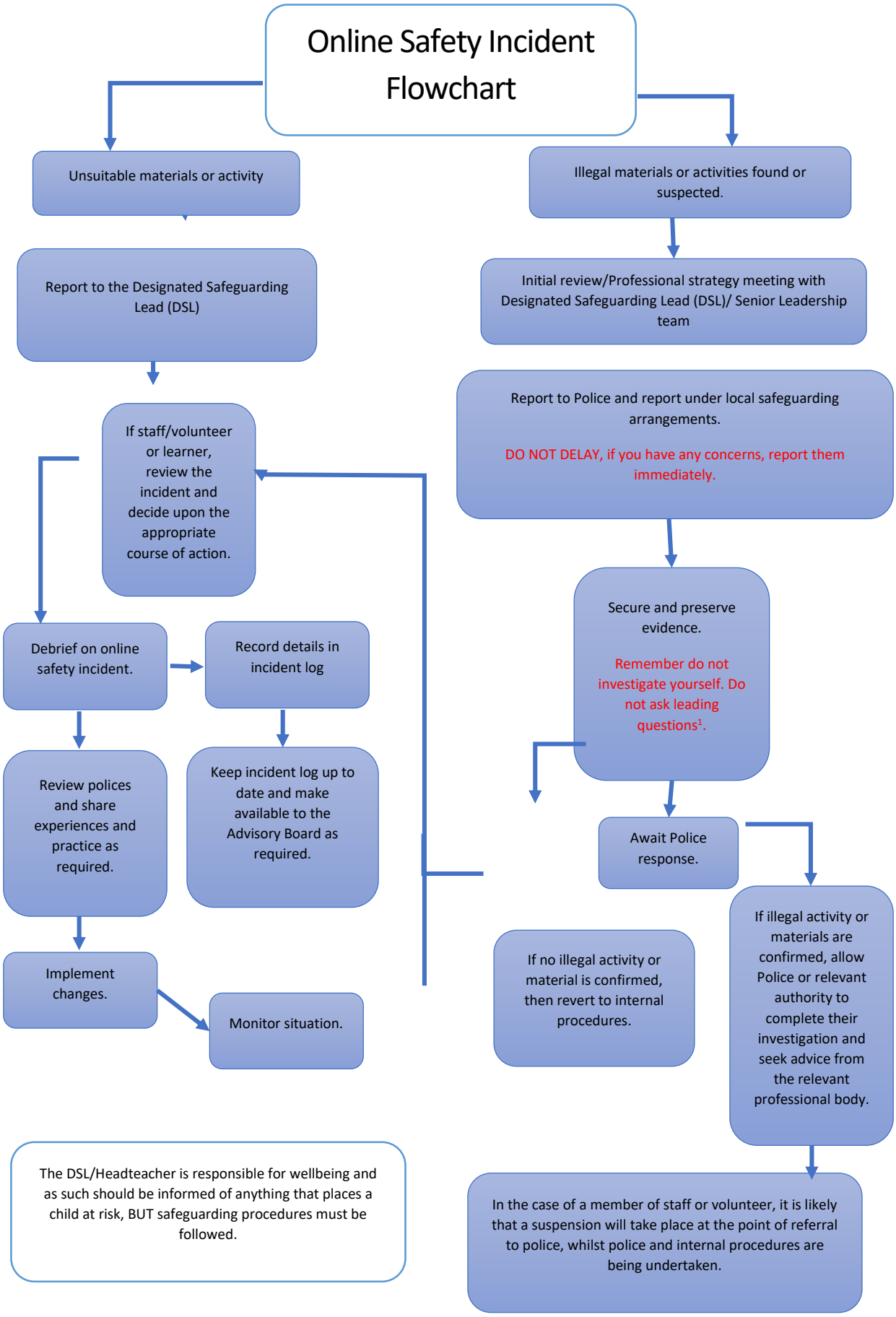
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged on CPOMs
- relevant staff should be 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
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:

    the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with

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

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

Online Safety Incident Flowchart



School actions

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

Responding to Learner Actions

Incidents	Refer to class teacher	Refer to school support manager	Refer to DSL/ Headteacher	Refer to Police/Social Work	Refer to IT Manager	Inform parents/carers	Remove device/ network/internet	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		x	x	x	x	x	x	x	x
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords			x	x	x	x	x	x	x
Corrupting or destroying the data of other users.			x	x	x	x	x	x	x
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x			x		x	x
Unauthorised downloading or uploading of files or use of file sharing.	x	x	x	x		x	x	x	x
Using proxy sites or other means to subvert the school's filtering system.	x	x	x	x	x	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	x	x	x	x	x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	x	x	x		x	x	x	x	x
Unauthorised use of digital devices (including taking images)	x	x	x	x	x	x	x	x	x
Unauthorised use of online services	x	x	x		x	x	x	x	x
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	x	x	x	x	x	x	x	x	x
Continued infringements of the above, following previous warnings or sanctions.									x

Responding to Staff Actions

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

Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	x					
Careless or intentional misuse of personal data (school, students or other members of the school community), e.g. displaying, holding or transferring data in an insecure manner	x				x	
Actions which could compromise the staff member's professional standing	x	x			x	x
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	x	x				x
Failing to report incidents whether caused by deliberate or accidental actions	x	x			x	x
Promoting a private business	x	x			x	x
Causing intentional damage to ICT facilities	x	x	x	x	x	x
Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel.	x	x	x	x	x	x
Continued infringements of the above, following previous warnings or sanctions.	x	x				x
Breeching the school's policies or procedures	x	x	x	x	x	x

These lists are not exhaustive. The school reserves the right to amend this list at any time. The Headteacher or Directors will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the ICT facilities.

Online Safety Education Programme

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways
A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and the SWGfL Project Evolve and regularly taught in a variety of contexts.

- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities
- vulnerability is actively addressed as part of a personalised online safety curriculum
- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the CyberChoices site.
- staff should act as good role models in their use of digital technologies the internet and mobile devices

- in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff are able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.
- a planned programme of formal online safety and data protection training will be made available to all learners

Contribution of Learners

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

- mechanisms to canvass learner feedback and opinion.
- appointment of digital leaders
- the Online Safety Group has learner representation
- learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns
- learners designing/updating Acceptable Use Agreements
- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

Staff/volunteers

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

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- the Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, and by reviewing guidance documents released by relevant organisations

- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the Designated Safeguarding Lead/IT manager (or other nominated person) will provide advice/guidance/training to individuals as required.

Advisors

Advisors should take part in online safety training/awareness sessions,
This may be offered in several ways such as:

- attendance at training provided by external agencies
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training will be made available to (at least) the Online Safety advisor. This will include:

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

Families

The school will seek to provide information and awareness to parents and carers through:

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

Technology

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

Filtering and Monitoring

The school filtering and monitoring provision is agreed by senior leaders, advisors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours
Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT Manager will have technical responsibility

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and an advisor with the involvement of the IT Service Provider.

- checks on the filtering and monitoring system are carried out by the IT Manager with the involvement of a senior leader, the Designated Safeguarding Lead and an advisor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or new technology is introduced e.g. using SWGfL Test Filtering

Filtering

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

- illegal content (e.g., child sexual abuse images) is filtered by the filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- staff will contact the IT Manager for requests/approvals for filtering changes
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
- younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle
- the school has guidelines around mobile technologies (see appendix)
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.
- the filtering provision should handle multi-lingual web content, images, common misspellings and abbreviations
- technologies and techniques that allow users to get around the filtering such as VPN's and proxy services should be identified and then blocked
- alerts should be provided when any web content has been blocked

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

Monitoring

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

- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead. All users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

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

- physical monitoring (adult supervision in the classroom)
- logging, regular monitoring and review of internet use
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts informing the school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitoring and recording the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)
- network monitoring using log files of internet traffic and web access

Role	**Responsibility**
Responsible Advisor	Strategic responsibility for filtering and monitoring and assurance that the standards are being met.
IT Manager	Team Member responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems
All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:	• they witness or suspect unsuitable material has been accessed • they can access unsuitable material • they are teaching topics which could create unusual activity on the filtering logs • there is failure in the software or abuse of the system • there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks • they notice abbreviations or misspellings that allow access to restricted material

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements. Responsibility for technical security resides with SLT who may delegate activities to identified roles.

- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT/Online Safety Group
- password policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)
- the security of their username and password and must not allow other users to access the systems using their log on details.
- **all school networks and system will be protected by secure passwords and multi-factor authentication wherever possible. Passwords must not be shared with anyone.**
- **the administrator passwords for school systems are kept in a secure place, e.g. school safe.**
- there is a risk-based approach to the allocation of user and learner usernames and passwords.
- passwords are immediately changed in the event of a suspected or confirmed compromise
- there will be regular reviews and audits of the safety and security of school technical systems including devices
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- The IT Manager is responsible for ensuring that all software purchased by and used by the school is adequately licensed and that the latest software updates (patches) are applied.
- The Director and IT manager is responsible for ensuring that software licencing logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed
- use of school devices out of school and by family members is regulated by an Acceptable Use Agreement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by an Acceptable Use Agreement that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the Headteacher/IT manager
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- by default, users do not have administrator access to any school owned device
- mobile device security and management procedures are in place (where mobile devices are allowed access to school systems).

- guest users are provided with appropriate access to school systems based on an identified risk profile.
- Cyber security is included in the school continuity plan
- Appropriate exit processes are implemented for devices no longer used. (Devices are wiped clean and then given to an appropriate company)

Mobile technologies

The school Acceptable Use Agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

The school allows:

	School devices			**Personal devices**		
	School owned for individual use	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes but in designated areas	Yes but in designated areas
Full network access	Yes	Yes	Yes	No(unless agreed by the Headteacher)	No	No
Internet only					Yes	Yes
Limited network access				Yes	Yes	Yes

School owned/provided devices

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

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

- The software /apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times.
- Where a school device has been provided to support learning it is expected that learners will bring devices to the school as required
- The changing of settings that would stop the device working as it was originally set up and intended to work is not permitted

Personal devices:

- there is a clear guidance covering the use of personal mobile devices on school premises for all users
- where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storage is made available.
- use of personal devices for school business is defined in the Acceptable Use Agreement and in the staff handbook. Personal devices commissioned onto the school network are segregated effectively from school-owned systems
- the expectations for taking/storing/using images/video aligns with the school's Acceptable Use Agreement. The non-consensual taking/using of images of others is not permitted.
- liability for loss/damage or malfunction of personal devices lies with the user and their parents / carers
- the school recommends that insurance is purchased to cover the device whilst out of the home
- the school accepts no responsibility for any malfunction of a device due to changes made to the device whilst on the school network or whilst resolving any connectivity issues
- the school recommends that the device is easily recognisable and has a protective case
- passcodes or pins should be set on any personal devices to aid security
- the school is not responsible for the day to day maintenance or upkeep of the users' personal device
- there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements
- education about the safe and responsible use of mobile devices is included in the school online safety education programmes
- personal devices are not permitted in tests or exams
- users are responsible for keeping their device up to date through software, security and app updates
- users are responsible for charging their own devices and for protecting and looking after their devices while in the school
- confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- printing from personal devices will not be possible

Electronic Devices - Searching Screening and Confiscation (updated with new DfE guidance – September 2022)

Introduction

Part 2 of the Education Act 2011 (Discipline) introduced changes to the powers afforded to schools by statute to search learners in order to maintain discipline and ensure safety. No such policy can on its own guarantee that the school will not face legal challenge but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).
The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question relates to an offence and/or may be used to cause harm, to disrupt teaching or could break the school rules.
Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so
The Headteacher must publicise the school behaviour policy, in writing, to staff, parents/carers and learners at least once a year.

Responsibilities
The Headteacher is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The Headteacher will need to authorise those staff who are allowed to carry out searches.
The Headteacher has authorised all DSLs, the IT Manager or all members of SLT to carry out searches for and of electronic devices and the deletion of data/files on those devices.

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

- at induction
- at regular updating sessions on the school's Online Safety policy

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data/files from those devices should receive training that is specific and relevant to this role.
Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Screening
The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data/files on those devices.
Learners are not allowed to bring mobile phones or other personal electronic devices into school (they are able to use them in the taxi on the way to and from school) or use them during the school day. If a personal device is being used in school as per reasonable adjustments which have been agreed by the Headteacher this device would need to have the same filtering and monitoring controls as school owned devices.
If learners breach these rules, authorised staff have the right to remove devices from bags and coats and add to the phone box that is locked under the stairs.

In carrying out the search:

- The authorised member of staff must have reasonable grounds for suspecting that a *learner* is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.
- The authorised member of staff should take reasonable steps to check the ownership of the mobile phone/personal electronic device before carrying out a search.
- The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the learner being searched.

- The authorised member of staff carrying out the search must be the same gender as the *learner* being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the *learner* being searched.
- There is a limited exception to this rule: Authorised staff can carry out a search of a learner of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:

- The person conducting the search may not require the learner to remove any clothing other than outer clothing.
- Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).
- 'Possessions' means any goods over which the learner has or appears to have control – this includes bags, coats and lockers.
- *A* learner's possessions can only be searched in the presence of the learner and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.
- The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.
- Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic Devices

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

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

Care of Confiscated Devices

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

Audit/Monitoring/Reporting/Review

The DSL and IT Manager will ensure that full records are kept of incidents involving the searching for and of electronic devices and the deletion of data/files.

These records will be reviewed by DSLs every week in their DSL meeting and advisors every half term in the Headteacher report.

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

The use of the internet, emails and social media sites has grown significantly and has vastly increased opportunities for teaching and learning. However, abuse of this technology, in terms of inappropriate use, has seen a significant increase in the number of disciplinary cases. This policy is written to apply to all employees in the school. The purpose of this policy is to ensure that:

- students and employees are safeguarded,
- the school is not exposed to legal risks,
- school employees have clear guidelines on what they can and cannot do to keep themselves safe and protected against allegations,
- teachers' use of the internet, email and social media sites does not conflict with the national teacher standards,
- the reputation of the school is not adversely affected by inappropriate use,
- Headteachers are able to manage conduct effectively.

Internet, Social Media and Email Use

Equal Opportunities and Scope

The school expects employees and volunteers working in the school to adhere to this policy in line with the school's obligations under equality legislation. The Headteacher must ensure that all reasonable adjustments or supportive measures are considered to allow equality of access and opportunity regardless

of age, gender, ethnicity, sexual orientation, disability, faith or religion, gender identity, pregnancy or marital status.

This policy should be read in conjunction with, and have due regard, to:

- ICT and Internet Acceptable Use Policy
- Discipline guidelines on conduct for employees (Code of Conduct)
- Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings
- The School's Anti-Bullying Policy

Through the implementation of this policy, the Directors will be mindful of the employer obligation to seek to maintain and protect the mental health and wellbeing of all staff as far as is reasonably practicable.

Internet use

The internet is a valuable resource for teaching and learning and is used regularly in school. However, it can also present a high level of risk if it is abused or if safe practices are not adopted.

Schools should advise employees not to use school equipment to access the internet for private purposes unless they have permission from the Headteacher. Employees should be made aware that the network and inappropriate use of the internet is closely monitored and individual usage can be traced - see paragraph 7 for further information. Inappropriate use of these facilities may constitute a criminal or disciplinary offence.

If employees or managers are unsure of what is or isn't appropriate use of the internet they can seek advice from the Online Safety Helpline by telephone on 0344 3814772 or by emailing helpline@saferinternet.org.uk.

Email use principles

- What is written in an email may have to be released under data protection law. Do not include information that may cause embarrassment, including to the school, maintain professionalism at all times.
- Always double-check that the email has been addressed to the correct recipient(s).
- If the e-mail concerns an individual, do not name them in the 'subject field'.
- Employee to student email communication must only take place via a school email account or from within the learning platform.
- Employees may only use approved e-mail accounts on the school system

Social media

Social media is the term commonly used for websites which allow people to interact with each other in some way (social networking) - by sharing information, opinions, knowledge and interests. Social media is part of many people's day to day lives. The following information has been put together for the benefit of employees to help them understand what may be deemed appropriate or inappropriate both inside and outside of work.

Communication via social media is rarely private. Employees should consider if it would not be said to a current or future colleague or parent, student or manager then it should not be published on a social media site, whether this is a school managed site or a personal one.

Online conduct should be as exemplary as offline conduct. Employees and volunteers must have regard to the fact that anything that is said on the internet could at some point be made public.

The school recognises that social media sites, websites and blogs provide a useful tool for communication and learning and are accessed widely. However, the safeguarding of students and employees is of paramount importance, adults should lead by example and set standards of behaviour. Therefore:

- Safeguarding of students and employees is the responsibility of all employees and this should also be taken into consideration when using personal social media sites inside and outside of the school. Employees should not link their own personal social media sites to anything related to the school.

- Employees are advised not to communicate with students or parents nor should they accept students or parents as friends on social media sites using their personal systems and equipment. Where a member of staff is related to a student the school should be made aware, if they are not already, and consideration given to whether any safeguards need to be put in place. Employees should also consider carefully the implications of befriending parents, carers or ex-students (over 18 years old or who have left the school at least two years ago) as contacts on social media sites.

- If employees use personal social media sites, they should not publish specific and detailed public thoughts or post anything that could bring the school into disrepute.

- Where employees are members of social media groups or pages (e.g. Facebook groups), whether private or public that refer to the school, any posts made in such groups should be in accordance with the school's policies.

- Employees must not place inappropriate photographs on any social media space and must ensure that background detail (e.g. house number, street name, school) cannot identify personal/employment details about them.

- Official blogs, microblogs (e.g. X), sites run by staff/the school must be password protected and overseen and sanctioned by the school.

- Contact should only be made with students for professional reasons via professional spaces set up and run by the school. If professional spaces are set up steps should be taken to ensure the users of the space are not put at risk e.g. privacy settings, data protection and data security. Permission should be sought from the Headteacher and the parents/guardians of students to communicate in this way.

- Employees are advised not to use or access the social media sites of students, without due reason e.g. safeguarding purposes.

- Cyberbullying of staff is not acceptable. The school has a separate policy for Cyberbullying. Please see this for what to do if this situation arises.

Monitoring and the consequences of improper/unacceptable use

Where the school believe unauthorised use of the information systems may be taking place, or the system may be being used for criminal purposes, then the decision may be taken to monitor the employee's use of the school's information systems e.g. email and/or internet use. Any monitoring will be conducted in accordance with a privacy impact assessment that the school has carried out to ensure that monitoring is

necessary and proportionate. Monitoring is in the school's legitimate interests and is to ensure that this policy on email and internet use is being complied with. See paragraph 5 for more information on data protection.

Under data protection law this type of monitoring is called 'occasional monitoring'. This is where the employer introduces monitoring as a short term measure to address a particular issue e.g. performance or conduct where concerns are of the nature explained above. Where monitoring takes place, schools must have due regard to article 8 of the European Convention on Human Rights, which means the employee still has a right to privacy in the workplace. This is the reason for the impact assessment, which should be carried out prior to any monitoring. Read the Employment Practice Guide on the Information Commissioner's Office (ICO) website, which provides an outline privacy impact assessment.

Employees must be aware that improper or unacceptable use of the internet or email systems could result in the use of the school's Disciplinary Procedure and, in some cases, legal proceedings. Sanctions will depend upon the gravity of misuse and could result in summary dismissal in some cases.

This policy relies on employees acting responsibly and in accordance with the outlined restrictions. Where employees have concerns that a colleague is acting in breach of the outlined restrictions, they are encouraged to raise this with the Headteacher or Chair of the Advisory Board/Directors if the concerns relate to the Headteacher.

If the concern involves possible inappropriate interaction between a colleague and a student, referral may be made to the designated senior professional in the school.

Legal Considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling Abuse

- When acting on behalf of the school, respond to harmful and / or offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of online communications, then this action must be reported using the agreed school protocols.

Use of Images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the school's digital and video images. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload learner pictures online other than via official school channels.
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Learners should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.

- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Parents/Carers

- If parents/carers have access to a platform where posting or commenting is enabled, parents/carers will be informed about Acceptable Use Agreement.
- The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
- Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

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

Managing your personal use of Social Media:

- Don't link your work email address to your social media accounts.
- Don't accept friend requests from parents/carers, current students or students who have the left the school less than two academic years previously on social media
- Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
- Don't make comments about your job, your colleagues, our school or our students. "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your privacy settings regularly and test your privacy
- Be careful about tagging other staff members in images or posts
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone

- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible
- Ensure the account is set up securely and the account can be transferred to another approved staff member in the event of the account holder leaving the school.

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Don't link to, embed or add potentially inappropriate content. Consider the appropriateness of content for any audience of school accounts.
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

When official school social media accounts are established, there should be:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal Use

personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy

- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- the school permits reasonable and appropriate access to personal social media sites during school hours e.g. break and lunch times

Monitoring of public social media

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

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

Digital and video images

The school will inform and educate users about these risks to reduce the likelihood of the potential for harm

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

When using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.

- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social media sites, nor should parents/carers comment on any activities involving other *learners* in the digital/video images
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy
- learners' work can only be published with the permission of the learner and parents/carers.

Online Publishing

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

- Public-facing website
- Social media
- Online newsletters

The school website is managed/hosted by Creative Corner. The school ensures that the Online Safety Policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

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

The school public online publishing provides information about online safety e.g., publishing the school's Online Safety Policy and Acceptable Use Agreements; curating latest advice and guidance; news articles etc., creating an online safety page on the school website.

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

Computer Misuse and Cyber Choices

All key stakeholders, including the school IT service providers, have responsibility for the safeguarding of young people from computer misuse and are aware of the Cyber Choices programme led by the National Crime Agency (NCA) and managed locally by Regional Organised Crime Units (part of the national policing network). The risks to young people of crossing the line into committing cybercrimes is a safeguarding issue.

All staff are made aware of the safeguarding risks of computer misuse.

All staff are familiar with the NCA Hacking it Legal Leaflet*, which explains Cyber Choices and the Computer Misuse Act 1990, and lists recommended resources for teachers to use.

Staff are aware of the role of their local Regional Organised Crime Unit as their point of contact for Cyber Choices referrals.

Learners agree to the Acceptable Use Policy (AUP) which outlines acceptable online behaviours and explains that some online activity is illegal. Acceptable computer use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the NCA Cyber Choices site.

Any breach of the AUP or activity by a learner that may constitute a cybercrime, in school or at home, will be referred to the Designated Safeguarding Lead for consideration as a safeguarding risk.

Where the DSL believes that the learner may be at risk of committing cybercrimes, or to already be committing cybercrimes, a referral to the local Cyber Choices programme will be made (contact details for all Regional Organised Crime Units are available in the "what to do if you're concerned" section at the bottom of the NCA Cyber Choices page). Where the DSL is unsure if a learner meets the referral criteria, advice should be sought from the local Cyber Choices team.

Parents also have the opportunity report potential cybercrime directly to the local Cyber Choices team but are recommended to make school-based concerns through the DSL.

The IT service provider is aware of the safeguarding requirement to refer concerns about computer misuse to the Designated Safeguarding Lead and has a clear process to follow in order to do so.

Information for parents about NCA Cyber Choices is available on the school website.

Data Protection

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

The school:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so

- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- has a Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice)
- has procedures in place to deal with the individual rights of the data subject
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

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

- data will be encrypted or password protected.
- device will be encrypted and password protected.
- device will be protected by up-to-date endpoint (anti-virus) software

- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Artificial intelligence

We understand the need to embrace emerging technology and recognise that AI-powered chatbots such as ChatGPT and Google Bard can produce impressive responses on a wide range of subjects. However, these large language models present a number of risks that cannot be ignored.

It is not our intention to impose a ban on using AI-powered chatbots to assist with work-related activities. In fact, we encourage their use where they can save time and expense.

Employees should be aware that the content inputted into an AI-powered chatbot may be used to train its model and could form part of the responses to questions posed by other users.

Employees are strictly prohibited from sharing personal data and special categories of personal data with any AI-powered chatbot, whether at work or in their own time

Personal data is any information that relates to a living individual who can be identified from that information.

Special categories of personal data means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

Any personal data and special categories of personal data must be handled in accordance with our data protection policy/policy on processing special categories of personal data.

Employees are also prohibited from inputting any information (either at work or in their own time) which identifies their place or work or specific school.

<u>Failure to comply with any of the above may result in disciplinary action being taken</u>.

Outcomes

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

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Advisors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendix

The appendices are as follows:

Learner Acceptable Use Agreement Template – (Years 7-11)
Learner Acceptable Use Agreement Template – (Year 5 and 6)
Learner Acceptable Use Agreement Template – for younger learners (Years 3 and 4)
Parent/Carer Acceptable Use Agreement Template
Staff (and Volunteer) Acceptable Use Policy Agreement Template
Online Safety Group Terms of Reference Template
Responding to incidents of misuse – flow chart
Reporting Log
Training Needs Audit Log
Staff laptop Usage Agreement
Student IT Equipment Loan Assessment
Legislation
Links to other organisations and resources
Glossary of Terms

Learner Acceptable Use Agreement Template – (Years 7-11)

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.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- 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 primarily 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.

I will act as I expect others to act toward me:

- 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 I am unable to use my own device in school
- 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 disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page 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 systems and devices.

Learner Acceptable Use Agreement Form

This form relates to the learner acceptable use agreement to which it is attached.

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 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 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, learning platform, website etc.

Name of Learner: .....

Group/Class: .....

Signed: .....

Date: .....

Parent/Carer Countersignature

Date:

Learner Acceptable Use Agreement Template – (Year 5 and 6)

Introduction

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.
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me.
- 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 by my teacher.

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- 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 am not allowed to use my personal device in school
- I will only use social media sites with permission and at the times that are allowed
- 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 do not follow these rules, I may be subject to consequences. This could include *loss of access to the school network/internet, detentions, suspensions, parents/carers contacted 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 systems.

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

- I use the school systems and devices (both in and out of school)
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: ..... Group/Class: .....

Signed: ..... Date: .....

Parent/Carer Countersignature

Date:

Learner Acceptable Use Agreement Template – (Year 3 and 4)

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 or suitable adult 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 or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult 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.

Signed (child): .....

Signed (parent): .....

Date:

Parent/Carer Acceptable Use Agreement Template

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/carers 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

Parent/Carers Name: .....

Learner Name: .....

As the parent/carer of the above learners, I give permission for my son/daughter to have access to the digital technologies at school.

Either: (Year 5 and above)

I know that my young person 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.

Or: (Year 3 and 4)

I understand that the school has discussed the Acceptable Use Agreement with my young person and that they have 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 young person'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.

Signed: .....

Date: .....

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Learners and membe may use chrome books, tablets or digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's first name will be used.

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

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their OWN children only at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social media sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children as specified below.

Digital/Video Images Permission Form

Parent/Carers Name:..... Learner Name:.....

As the parent/carer of the above learner, I agree to the school taking digital/video images of my child/children.	Yes/No	
I agree to these images being used:		
• to support learning activities within school, eg. school display boards	Yes/No	With child's first name? Yes/No
• in publicity that celebrates success and promotes the work of the school, including: school brochures, school website, the press, X (formerly Twitter) and other public/external media.	Yes/No	With child's first name? Yes/No
I agree to use of my child's first name ONLY.	Yes/No	
I agree that I may only take digital or video images at/of school events of **my own child/children only** and to abide by these guidelines in the use of these images.	Yes/No	

Signed: .....

Date: .....

ALL SAINTS SCHOOL
School Road, Lessingham, Norwich, Norfolk
NR12 0DJ
01692 582083
www.allsaintslessingham.co.uk
E-mail: office@allsaintslessingham.co.uk

ACHIEVEMENT FOR ALL

G Suite for Education Notice to Parents and Carers

Dear Parents and Carers

To ensure the online safety of our students, we are using Securly (cloud-based web filter company) which works alongside G Suite to offer cloud-based web filtering. All internet searches and activity is monitored internally by the Securly Administrators and Safeguarding Team. Any searches of concern are reported directly to the Headteacher. Securly also enables us to audit emails, documents and Drive for any instances of cyber-bullying, violence, concerning activity or any other instance which would require further action from the school.

This notice describes the personal information we provide to Google for these accounts and how Google collects, uses, and discloses personal information from students in connection with these accounts.

Using their G Suite for Education accounts, students may access and use the following "Core Services" offered by Google (described at https://gsuite.google.com/terms/user_features.html):

- Gmail
- Google+
- Calendar
- Chrome Sync
- Classroom
- Cloud Search
- Contacts
- Docs, Sheets, Slides, Forms
- Drive
- Groups
- Hangouts, Hangouts Chat, Hangouts Meet, Google Talk
- Jamboard
- Keep
- Sites
- Vault

In addition, we also allow students to access certain other Google services with their G Suite for Education accounts. Specifically, your child may have access to the following "Additional Services":

- YouTube, Blogger, Google Maps (A list of additional services is available)
- These can be Apps which have been specifically chosen by the school and have educational value and relevance to teaching.

Google provides information about the information it collects, as well as how it uses and discloses the information it collects from G Suite for Education accounts in its G Suite for Education Privacy Notice. You can read that notice online at https://gsuite.google.com/terms/education_privacy.html You should review this information in its entirety, but below are answers to some common questions:

What personal information does Google collect?

When creating a student account, All Saints School may provide Google with certain personal information about the student, including, for example, a name, email address, and password, which are held securely on our own server.

- log information, including details of how a user used Google services, device event information,
- and the user's Internet protocol (IP) address;
- location information, as determined by various technologies including IP address, GPS, and
- other sensors;
- unique application numbers, such as application version number; and
- cookies or similar technologies which are used to collect and store information about a browser or device, such as preferred language and other settings.

How does Google use this information?

In G Suite for Education Core Services, Google uses student personal information to provide, maintain, and protect the services. Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes.

In Google Additional Services, Google uses the information collected from all Additional Services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and its users. Google may also use this information to offer tailored content, such as more relevant search results. Google may combine personal information from one service with information, including personal information, from other Google services.

Does Google use student personal information for users in KS1 and KS2 schools to target advertising?

No. For G Suite for Education users in primary and secondary (K-12) schools, Google does not use any user personal information (or any information associated with an G Suite for Education Account) to target ads, whether in Core Services or in other Additional Services accessed while using an G Suite for Education account.

Can my child share information with others using the G Suite for Education account?

We may allow students to access Google services such as Google Docs and Sites, which include features where users can share information with others or publicly. When users share information publicly, it may be indexable by search engines, including Google.

Will Google disclose my child's personal information?

Google will not share personal information with companies, organisations and individuals outside of Google unless one of the following circumstances applies:

- With parental or guardian consent. Google will share personal information with companies, organisations or individuals outside of Google when it has parents' consent (for users below the age of consent), which may be obtained through G Suite for Education schools.
- With All Saints School, G Suite for Education accounts, because they are school managed accounts, give administrators access to information stored in them.

- For external processing. Google may provide personal information to affiliates or other trusted businesses or persons to process it for Google, based on Google's instructions and in compliance with the G Suite for Education privacy notice and any other appropriate confidentiality and security measures.
- For legal reasons. Google will share personal information with companies, organizations or individuals outside of Google if it has a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:
    - meet any applicable law, regulation, legal process or enforceable governmental request.
    - enforce applicable Terms of Service, including investigation of potential violations.
    - detect, prevent, or otherwise address fraud, security or technical issues.
    - protect against harm to the rights, property or safety of Google, Google users or the public as required or permitted by law.

Google also shares non-personal information -- such as trends about the use of its services --publicly and with its partners.

What choices do I have as a parent or guardian?

First, you can consent to the collection and use of your child's information by Google. If you don't provide your consent, we will not continue to provide a G Suite for Education account for your child, and Google will not collect or use your child's information as described in this notice.

If you consent to your child's use of G Suite for Education, you can access or request deletion of your child's G Suite for Education account by contacting the school office. If you wish to stop any further collection or use of your child's information, you can request that we use the service controls available to limit your child's access to features or services, or delete your child's account entirely. You and your child can also visit https://myaccount.google.com while signed in to the G Suite for Education account to view and manage the personal information and settings of the account.

What if I have more questions or would like to read further?

If you have questions about our use of Google's G Suite for Education accounts or the choices available to you, please contact the school office. If you want to learn more about how Google collects, uses, and discloses personal information to provide services to us, please review the G Suite for Education Privacy Centre (at https://www.google.com/edu/trust/), the G Suite for Education Privacy Notice (at https://gsuite.google.com/terms/education_privacy.html), and the Google Privacy Policy (at https://www.google.com/intl/en/policies/privacy/).

The Core G Suite for Education services are provided to us under Google's Apps for Education agreement (at https://www.google.com/apps/intl/en/terms/education_terms.html).

ALL SAINTS SCHOOL
School Road, Lessingham, Norwich, Norfolk
NR12 0DJ
01692 582083
www.allsaintslessingham.co.uk
E-mail: office@allsaintslessingham.co.uk

ACHIEVEMENT FOR ALL

G Suite for Education consent form

Dear Parents and Carers

At All Saints School, we are using G Suite for Education, and we are seeking your permission to provide and manage a G Suite for Education account for your child. G Suite for Education is a set of education productivity tools from Google including Gmail, Calendar, Docs, Classroom, and more used by tens of millions of students and teachers around the world. At All Saints School, students will use their G Suite accounts to complete work, communicate with their teachers, and sign into Chromebooks.

The Google and G Suite Privacy Notice https://gsuite.google.com/terms/education_privacy.html provides answers to common questions about what Google can and can't do with your child's personal information, including:

- What personal information does Google collect?
- How does Google use this information?
- Will Google disclose my child's personal information?
- Does Google use student personal information for users in KS1 and KS2 schools to target advertising?
- Can my child share information with others using the G Suite for Education account?

Please read it carefully, let us know of any questions, and then sign below to indicate that you've read the notice and give your consent. If you don't provide your consent, we will no longer provide a G Suite for Education account for your child.

Yours sincerely

Ms Sam Dangerfield
Headteacher

G Suite for Education consent form

I give permission for All Saints School to create/maintain a G Suite for Education account for my child and for Google to collect, use, and disclose information about my child only for the purposes described in the Google and G Suite Privacy Notice.

Full name of student _____

Printed name of parent/carer _____

Signature of parent/carer _____

Date _____

Staff (and Volunteer) Acceptable Use Policy Agreement Template

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, learning platform 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 staff members' 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/learning platform /social media) it will not be possible to identify by full name, or other personal information, those who are featured.
- I will only use social media 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 programs)
- 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 programs 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 programs 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 Advisors / Directors 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: .....

School Policy Template – Online Safety Group Terms of Reference

1. Purpose

To provide a consultative group that has wide representation from All Saints School community, with responsibility for issues regarding online safety and the monitoring of the Online Safety Policy including the impact of initiatives.

2. Membership

The online safety group will seek to include representation from all stakeholders.

The composition of the group should include :

- Headteacher and Designated Safeguarding Lead (DSL)
- IT Manager who is also the Online Safety Lead (OSL)
- Advisor
- School secretary
- Teacher and or Support staff member
- Parent/Carer
- Learners

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

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

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

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

3. Chairperson

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

- Scheduling meetings and notifying members;
- Inviting other people to attend meetings when required
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. Duration of Meetings

Meetings shall be held twice a year for a period of 1 hour.

5. Functions

These are to assist the DSL/IT Manager (or other relevant person) with the following:

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the Online Safety Policy in line with new technologies and incidents
- To monitor the delivery and impact of the Online Safety Policy

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

6. Amendments

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

Signed by (HT): ..... Date: .....

Date for review: .....

Laptop Usage Policy and Agreement

This policy outlines the responsibilities that staff must accept when they are issued a laptop. It applies to all members of staff who have been issued with a laptop, or the use of a laptop, from the school.
Any member of staff issued with a/with use of a laptop will need to confirm, by signing an acceptance of the policy, that he/she has read, understands and will comply with the policy. A copy of the policy will need to be signed by the member of staff, with a copy being retained in school until the laptop is returned or replaced. When a member of staff is provided with a laptop, he/she accepts responsibility for safeguarding the laptop itself as well as the data stored on the laptop.

All laptops issued to staff will be checked by a person appointed by the Directors on a monthly basis to ensure proper use.

- I agree that the laptop at all times remains the property of All Saints School (Lessingham) Limited and that the laptop is provided for my use as a teacher to assist me in developing educational learning materials, assessment reporting and any other appropriate actions relevant to my position at All Saints School.
- I may use the laptop for the duration of my employment or until my role changes and I no longer require use of a laptop.
- I undertake to keep the laptop in good working order and to notify Rachel Smith or the Headteacher of any defect or malfunction of the laptop while in my care.
- I will not sell, assign, transfer or otherwise dispose of the laptop.
- I will not remove, conceal or alter any laptop package markings or tags or engrave or mark the laptop in any way that will reduce the value of the laptop.
- I will take due care of the laptop package at all times, including (but not limited to)
    - Ensure I have appropriate car and house insurance to be able to transport/use the laptop at home (the laptop is also covered under the insurance policy of All Saints School).
    - Not leaving the laptop unattended in a public place.
    - Not leaving the laptop unattended or unsecured in a classroom or other place in school.
    - Not leaving the laptop in plain view in an unattended or unsecured vehicle.
    - Not allowing the laptop to be accessed by any other person (unless authorised by All Saints School).
    - Not allowing the laptop to be interfered with, tampered with or altered by a third party.
    - Ensuring due care is taken in the handling, transporting and usage of the laptop.
    - Not using the laptop in environments that might increase the likelihood of damage.
- Any damage or loss must be reported to the Headteacher and Directors as soon as possible and the police in cases of theft.
- I will keep an independent record of the laptop serial number (included on this agreement) that I will use if need to report theft of the laptop to the police.
- I understand that I will not be held responsible for computer problems resulting from regular school-related use, but may be held responsible for any problems caused by my negligence as deemed by the Directors.
- I will not work on or save sensitive information (e.g. education records, personally identifiable information and confidential information) without taking proper precautions
- I will never leave the laptop unattended and logged on. Always shut down, log off or lock the screen before walking away from the machine
- I will upload all my files to the staff S: Drive to ensure no loss of data.

- I understand that the laptop has anti-virus software installed and I will keep this up to date and enabled.
- I will not open any email or attachment unless it is expected and from a legitimate source.
- I will report any security incidents (such as virus infections) to the Headteacher immediately in order to minimise the risk to the school.
- I will not download, install or use unauthorised software programmes. No personal programmes are to be used, e.g. iTunes.
- Any software that is required in addition to that provided with the laptop must first be approved by the Directors to ensure the correct permissions and licences are in place.
- I will make the laptop available on request of either the Directors or Headteacher for updates and any alterations to system setup.
- All members of staff are accountable for all network and systems access under their individual user ID. Passwords should be kept absolutely secret and should never be shared with anyone unless required by All Saints School for maintenance of the laptop.
- Laptops are provided for official use by authorised employees. All Saints School (Lessingham) Limited laptops must not be loaned or allowed to be used by others.
- I will comply with relevant laws, regulations and policies applying to the use of computers and information, e.g. licence, copyright, GDPR.
- All Saints School will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, photographs, videos or e-mail messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the laptop.

Failure to comply with this policy could lead to disciplinary action.

Items Loaned/Condition

Item	Loaned		Condition	
Laptop Computer	Yes	No	New	Used
Power Supply and Cord	Yes	No	New	Used
Mouse and USB	Yes	No	New	Used
Laptop Case	Yes	No	New	Used

Comments: (overall condition, scratches, dents etc.)

Laptop Make and Model: _____

Laptop Serial Number: _____

Employee name (please print): _____

Employee signature: _____

Date: _____

Student IT Equipment Loan Assessment

1. This agreement is between:
1) All Saints School (Lessingham) Limited ("the school")
2) [Name of parent and their address] ("the parent" and "I")
and governs the use and care of devices assigned to the parent's child (the "student"). This agreement covers the period from the date the device is issued through to the return date of the device to the school. All issued equipment shall remain the sole property of the school and is governed by the school's policies.
1. The school is lending the student a Chromebook ("the equipment") for the purpose of attending and completing online lessons and set school
2. This agreement sets the conditions for taking an All Saints School Chromebook home.
I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the student will adhere to the terms of loan.

2. Damage/loss
By signing this agreement, I agree to take full responsibility for the loan equipment issued to the student and I have read or heard this agreement read aloud and understand the conditions of the agreement.
I understand that I and the student are responsible for the equipment at all times whether on the school's property or not.
If the equipment is damaged, lost or stolen, I will immediately inform Miss King (kking@allsaintslessingham.co.uk) and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

I will make sure my child takes the following measures to protect the device:

- Keep the device in a secure place when not in use
- Don't leave the device in a car or on show at home
- Don't eat or drink around the device
- Don't lend the device to siblings or friends
- Don't leave the equipment unsupervised in unsecured areas

3. Unacceptable use
I am aware that the school monitors the student's activity on this device.
I agree that my child will not carry out any activity that constitutes 'unacceptable use'.
This includes, but is not limited to the following:

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Causing intentional damage to ICT facilities or materials
- Using inappropriate or offensive language
- Searching for or viewing inappropriate material

I accept that the school will sanction the student, in line with our behaviour/discipline policy, if the student engages in any of the above **at any time.**

4. Personal use
I agree that the student will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person. The equipment can only be used for the purposes of education during the hours of 9.00am-3.15pm and for completing set school work out of these hours.

5. Data protection
I agree to take the following measures to keep the data on the device protected.

- Keep the equipment password-protected – the password for the pupil logging in has been set by the school and no attempt must be made to change this. If the password has been forgotten, please contact Miss King.
- Make sure my child locks the equipment if it's left inactive for a period of time
- Do not share the equipment among family or friends

If I need help doing any of the above, I will contact Miss King on the email kking@allsaintslessingham.co.uk

6. Return date
I will return the device in its original condition to Miss King within 7 days of being requested to do so.
I will ensure the return of the equipment to the school if the student no longer attends the school.

7. Consent
[If parents are collecting the equipment]
By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

STUDENT'S Full name	
PARENT'S Full name	
PARENT'S signature	

[If a signed physical copy is not able to be obtained]
By signing this form, I confirm that I have read and agree to the terms and conditions set out above.
Please sign by typing your name and your child's name.

STUDENT'S Full name	
PARENT'S full name	

Reporting log

Date of issue	Date reported	Initials of User	Reported by	Report method	Filter or Aware

Training Needs Audit Log

Training Needs Audit Log Group:				
Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

Appendix One

Mobile devices in school

All Saints School has a firm policy that NO mobile devices – phones, iPads, Kindles, tablets etc – are allowed in school.

If your child brings such a mobile device to school (eg. for use on the journey), this MUST be handed in on arrival and before entering the school. There are no exceptions to this school rule.

A storage box is provided for all devices, which is kept securely locked away for the duration of the school day. Students may then collect their device at the end of the school day as they proceed to their transport home.

Any student bringing in a device does so entirely at their own risk and on the understanding that All Saints School accepts no responsibility for any malfunction, loss or damage to said device.

Legislation

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

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

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

Computer Misuse Act 1990

This Act makes it an offence to:

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

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

Data Protection Act 1998

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

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

The Data Protection Act 2018:

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

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.

- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

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

Freedom of Information Act 2000

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

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

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

Regulation of Investigatory Powers Act 2000

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

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

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

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

Telecommunications Act 1984

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

Criminal Justice & Public Order Act 1994

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

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

Racial and Religious Hatred Act 2006

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

Protection from Harassment Act 1997

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

Protection of Children Act 1978

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

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

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

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

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

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

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

The Education and Inspections Act 2006

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

The Education and Inspections Act 2011

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

See template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/learnersupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

The Protection of Freedoms Act 2012

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

The School Information Regulations 2012

Requires schools to publish certain information on its website:

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

Serious Crime Act 2015

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

Criminal Justice and Courts Act 2015

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

For further guidance or support please contact the Revenge Porn Helpline

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/
Harmful Sexual Support Service

CEOP

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

Others

LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Tools for Schools / other organisations

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self-review tool: www.360data.org.uk
SWGfL Test filtering - http://testfiltering.com/
UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework
SWGfL 360 Groups – online safety self review tool for organisations working with children
SWGfL 360 Early Years - online safety self review tool for early years organisations

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
SELMA – Hacking Hate - https://selma.swgfl.co.uk
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking
Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum
SWGfL Evolve - https://projectevolve.co.uk
UKCCIS – Education for a connected world framework
Department for Education: Teaching Online Safety in Schools
Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Data Protection
360data - free questionnaire and data protection self review tool
ICO Guides for Organisations
IRMS - Records Management Toolkit for Schools
ICO Guidance on taking photos in schools

Professional Standards/Staff Training
DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet – School Pack for Online Safety Awareness
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support/Cyber-security
UKSIC – Appropriate Filtering and Monitoring
SWGfL Safety & Security Resources
Somerset - Questions for Technical Support
SWGfL - Cyber Security in Schools.
NCA – Guide to the Computer Misuse Act
NEN – Advice and Guidance Notes

Working with parents and carers
SWGfL – Online Safety Guidance for Parents & Carers
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters

Prevent
Prevent Duty Guidance
Prevent for schools – teaching resources
Childnet – Trust Me

Research
Ofcom –Media Literacy Research
Ofsted: Review of sexual abuse in schools and colleges

Glossary of Terms

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

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