

The Priory CE VA Primary School

Inspiring a generation to learn, flourish and achieve in a caring, Christian community.



Online Safety Policy

Online Safety Policy			
Approval	Board of Governors	Chair	Geoff Tabor
Headteacher	Sarah Richardson	Ratified	June 2024
Date of Last Review	July 2023	Date of This Review	February 2024
Date of Next Review	February 2025	Maintenance	Headteacher

February 2024	Full policy rewrite by MM utilising template from SWGfL based on latest safeguarding guidance.
---------------	--

Contents

Contents	2
1. Policy Purpose	3
2. Roles and Responsibilities	4
3. Acceptable Use	6
3.1 Acceptable Use Agreements (AUAs)	6
3.2 Unacceptable User Actions	6
3.3 Other User Activities	7
3.4 Appropriate Use of Communication Technologies	8
4. Reporting and Responding to Online Safety Incidents	9
4.1 Reporting and Responding Principles	9
4.2 Reporting and Responding Procedure	11
4.3 Responding to Pupil Misuse	12
4.4 Responding to Staff Misuse	13
5. Online Safety Education	15
5.1 Online Safety Education for Pupils	15
5.2 Online Safety Education for Staff	15
5.3 Online Safety Education for Governors	16
5.4 Online Safety Education for Parents / Carers	16
6. Technology Infrastructure	17
6.1 Technical Security	17
6.2 Filtering and Monitoring	18
6.2.1 Filtering	18
6.2.2 Monitoring	18
6.3 Password Security	19
6.3.1 Password Principles	19
6.3.2 Learner Passwords	19
6.4 Mobile Technology	20
6.4.1 Permitted Mobile Devices	20
6.4.2 Searching, Screening and Confiscation	20
7. Social Media	22
7.1 Staff Use of Social Media	22
7.2 School Social Media Accounts	23
7.3 Monitoring of Public Social Media	23
8. Online Publishing	23
9. Digital and Video Images	24
Appendix 1: Loaned Device Indemnity Form	25
Appendix 2: Acceptable Use Agreement - EY/KS1 Pupils	26
Appendix 3: Acceptable Use Agreement - KS2 Pupils	27
Appendix 4: Acceptable Use Agreement - SEND Pupils	29
Appendix 5: Acceptable Use Agreement - Parents	31
Appendix 6: Acceptable Use Agreement for Staff	32
Appendix 7: Acceptable Use Agreement for Visitors	34

1. Policy Purpose

The school recognises the benefits of access to digital technology, as well as risks that may be associated with this:

- Content: Being exposed to illegal, inappropriate or harmful content.
- Contact: Being subjected to harmful online interaction with other users.
- Conduct: Online behaviour that increases the likelihood of, or causes, harm.
- Commerce: Risks with a financial or contractual element.

This Online Safety Policy outlines the commitment of The Priory CE VA Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.

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.
- 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.

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

2. Roles and 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	Designated Safeguarding Lead (DSL)
<ul style="list-style-type: none"> ● hold duty of care for ensuring the safety of members of the school community and fostering a culture of safeguarding ● have an awareness of procedures to be followed in the event of a serious online safety allegation being made against a member of staff ● ensure relevant staff carry out their responsibilities effectively and receive appropriate training ● ensure there is a system in place to allow for monitoring and the receipt of regular reports 	<ul style="list-style-type: none"> ● hold lead responsibility for online safety ● (with the OSL) be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded
Online Safety Lead (OSL)	Governing Body: Safeguarding Governor
<ul style="list-style-type: none"> ● receive relevant and regularly updated training in online safety ● meet regularly with the Safeguarding Governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs ● ensure (at least annually) annual filtering and monitoring checks are carried out ● (with the DSL) be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded ● liaise with staff and IT providers on matters of safeguarding and welfare ● establish and review the online safety policy, taking into account online safety incidents and changes, trends in technology and related behaviours ● promote an awareness of and commitment to online safety ● ensure that the online safety curriculum is planned, mapped, embedded and evaluated 	<ul style="list-style-type: none"> ● approve the Online Safety Policy and reviewing its effectiveness ● regularly meet the DSL / OSL ● regularly receive (collated and anonymised) reports of online safety incidents ● check that provision outlined in the Online Safety Policy is taking place as intended ● ensure that filtering and monitoring provision is reviewed and recorded at least annually ● report to the broader governing body ● receive cyber-security training to enable the governors to check that the school meets the DfE Cyber Security Standards

<ul style="list-style-type: none"> ● ensure that all staff are aware of the procedures to be followed in the event of an online safety incident ● provide training and advice for staff, governors, parents/carers and pupils ● ensure that online safety provision is regularly reviewed, including through the 360-degree safe self-review tool 	
Teaching and Support Staff	IT Provider
<ul style="list-style-type: none"> ● have an awareness of current online safety matters / trends and of the school Online Safety Policy ● understand that online safety is a core part of safeguarding ● read, understand and sign the staff acceptable use agreement (AUA) ● report any suspected misuse or problem, in line with the school safeguarding procedures ● ensure all digital communications are on a professional level and only carried out using official school systems ● ensure learners understand and follow the Online Safety Policy and AUAs ● supervise and monitor the use of digital technologies ● check planned online content is suitable ● model safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media 	<p><i>under the direction of the senior leadership team</i></p> <ul style="list-style-type: none"> ● have an awareness of and follow the school Online Safety Policy ● ensure the school technical infrastructure is secure and not open to misuse or malicious attack ● ensure the school meets the required online safety technical requirements as identified by the <u>DfE Meeting Digital and Technology Standards in Schools & Colleges</u> ● ensure there is clear, safe and managed control of user access to networks and devices ● keep up to date with online safety technical information ● ensure the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the OSL/DSL ● support the OSL in ensuring the regular review of the filtering and monitoring system
Pupils	Parents and Carers
<ul style="list-style-type: none"> ● use digital technology in accordance with the pupil AUA and Online Safety Policy ● understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so ● know what to do if they or someone they know feels vulnerable when using online technology ● understand the importance of adopting good online safety practice outside of school 	<p><i>with the support of the school leadership through the publication of the Online Safety Policy, the sharing of AUAs, and the provision of guidance and training</i></p> <ul style="list-style-type: none"> ● reinforce the online safety messages provided to learners in school ● use digital technology in accordance with the parent/carer AUA and Online Safety Policy

3. Acceptable Use

3.1 Acceptable Use Agreements (AUAs)

The Online Safety Policy and acceptable use agreements (AUAs) define acceptable use at the school. The AUAs (see appendices) will be communicated and reinforced through the staff handbook, posters/notices, communication with parents/carers, annual refresher training and agreement, the school's curriculum, and the school website.

3.2 Unacceptable User Actions

Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse imagery
- Child sexual abuse/exploitation/grooming
- Terrorism
- Encouraging or assisting suicide
- Offences relating to sexual images i.e., revenge and extreme pornography
- Incitement to and threats of violence
- Hate crime
- Public order offences - harassment and stalking
- Drug-related offences
- Weapons / firearms offences
- Fraud and financial crime including money laundering

Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act:

- 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)

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
- Promotion of any kind of discrimination
- Using school systems to run a private business
- Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school

- Infringing copyright
- Unfair usage (downloading/uploading large files that hinders others in their use of the internet)
- 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

3.3 Other User Activities

Action	Staff and Other Adults	Learners
online gaming	✗	☐ only educational games approved by SLT
online shopping/commerce	☐ only for school purchases	✗
file sharing	☐ only using school file sharing / storage systems	☐ only using school file sharing / storage systems
social media	☐ only using school accounts by members of SLT; or using personal devices in the staff room	✗
messaging/chat	☐ only using school systems; or using personal devices in the staff room	✗
entertainment streaming, e.g. Netflix, Disney+	☐ only for classroom purposes, with SLT approval	✗
use of video broadcasting, e.g. YouTube, Twitch, Tiktok	☐ YouTube for learning purposes, only watching (not broadcasting) appropriate, pre-checked content	☐ only when shown something by a member of staff (see left)
use of mobile phones in school	☐ only used by SLT for school purposes; or in the staff room	✗ Y5/6 who bring devices should hand these in
taking photos on mobile phones	☐ only used by SLT for school purposes and with immediate deletion	✗
use of other personal devices, e.g. tablets, gaming devices	✗	✗
use of personal email on school network/wi-fi	☐ only in the staff room and using public wi-fi	✗
use of school email for personal emails	✗	✗
✗ unacceptable action ☐ action acceptable in certain situations ✓ acceptable action		

3.4 Appropriate Use of Communication Technologies

The school values the effective use of communication technology in conducting its activities. In the school, the following means of communication are utilised:

- Telephone - For contact between professionals and with parents/carers.
- Email - For contact between professionals and with parents/carers (parent/carer communication is conducted via the school office email account).
- Google Classroom - For contact between staff and pupils (and their parents/carers).
- Social Media - For contact between senior staff and the school community.

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 (email, social media, learning platform, etc.) must be professional in tone and content. Personal email 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 (see social media section of this policy).
- Users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school email addresses should be used to identify members of staff and learners.

4. Reporting and Responding to Online Safety Incidents

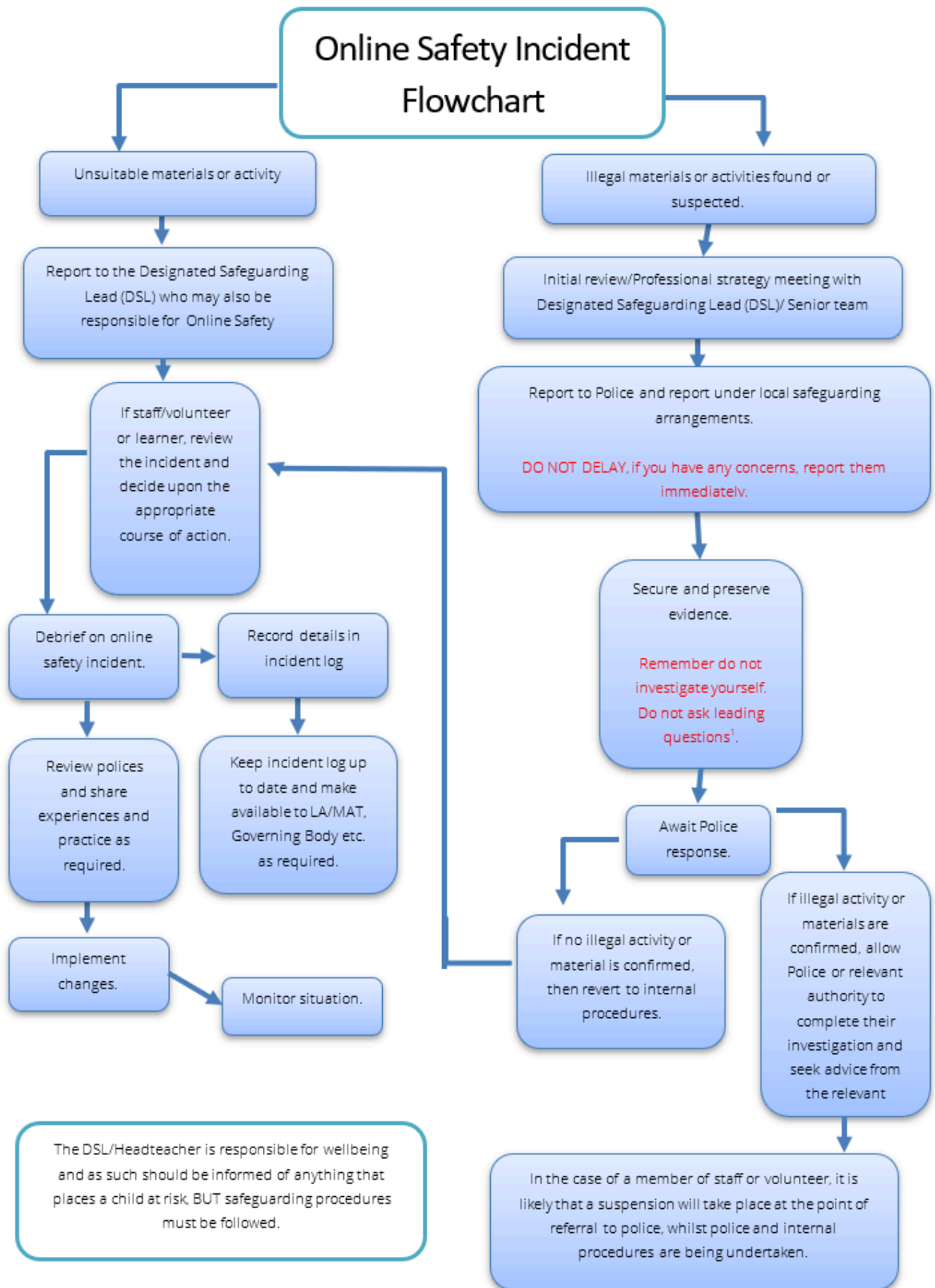
4.1 Reporting and Responding Principles

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 ensures:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies. Staff make use of the CPOMs system to record safeguarding concerns, and pupils are taught to 'tell a trusted adult', and have access to boxes where they can share information with teachers. It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- All members of the school community are made aware of the need to report online safety issues/incidents.
- Reports will be dealt with as soon as is practically possible once they are received.
- The Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; [Professionals Online Safety Helpline](#); [Reporting Harmful Content](#); [CEOP](#).
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures. This may include:
 - non-consensual images
 - self-generated images
 - terrorism / extremism
 - hate crime / abuse
 - fraud and extortion
 - harassment / stalking
 - Child Sexual Abuse Material (CSAM)
 - Child Sexual Exploitation Grooming
 - extreme pornography
 - sale of illegal materials / substances
 - cyber or hacking [offences under the Computer Misuse Act](#)
 - copyright theft or piracy
- Any concern about staff misuse is reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority / MAT, in line with the school's safeguarding policy.

- Where there is no suspected illegal activity, devices may be checked using the following procedures:
 - One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
 - Conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
 - Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
 - Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form.
 - Once this has been completed and fully investigated, the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - internal response or discipline procedures
 - involvement by local authority / MAT (as relevant)
 - police involvement and/or action
- Learning from the incident (or pattern of incidents) is provided (as relevant and anonymously) to staff responsible for online safety, the broader staff team, pupils, parents/carers, governors, and local authorities/external agencies as appropriate.

4.2 Reporting and Responding Procedure



4.3 Responding to Pupil Misuse

The agreed response to incidents of misuse will be implemented through normal behaviour procedures, and, although the outcome may vary depending on the nature and severity of the incident, may include the following:

	Refer to HT / SLT	Refer to Police / Social Services	Refer to Technical Support for Advice / Action	Inform Parents / Carers	Further Sanction in Line with Behaviour Policy
Deliberately accessing or trying to access material that could be considered illegal.	✓	✓	✓	✓	✓
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access the school network by sharing username and passwords.	✓		✓	✓	✓
Corrupting or destroying the data of other users.	✓		✓	✓	✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature.	✓			✓	✓
Unauthorised downloading or uploading of files or use of file sharing.	✓		✓	✓	✓
Using proxy sites or other means to subvert the school's filtering system.	✓		✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident.	✓		✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material.	✓		✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	✓			✓	
Unauthorised use of digital devices (including taking images).	✓			✓	
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	✓			✓	✓
Continued infringements of the above, following previous warnings or sanctions.	✓	✓	✓	✓	✓

4.4 Responding to Staff Misuse

The agreed response to incidents of misuse will be implemented through normal disciplinary procedures, and, although the outcome may vary depending on the nature and severity of the incident, may include the following:

	Refer to HT / SLT	Refer to Local Authority	Refer to Police	Refer to Technical Support for Advice / Action	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal	✓	✓	✓	✓	✓
Deliberate actions to breach data protection or network security rules.	✓	✓		✓	✓
Deliberately accessing or trying to access offensive or pornographic material.	✓	✓		✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.	✓	✓	✓	✓	✓
Using proxy sites or other means to subvert the school's filtering system.	✓	✓		✓	✓
Unauthorised downloading or uploading of files or file sharing.	✓	✓		✓	✓
Breaching copyright or licensing regulations.	✓	✓			✓
Allowing others to access school networks by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	✓	✓		✓	✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature.	✓	✓			✓
Using personal email/social networking/messaging to carry out digital communications with learners and parents/carers.	✓	✓			✓
Inappropriate personal use of digital technologies, e.g. social media / personal email.	✓	✓			✓
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner.	✓	✓		✓	✓

Actions which could compromise the staff member's professional standing.	✓	✓			✓
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	✓	✓			✓
Failing to report incidents whether caused by deliberate or accidental actions.	✓	✓			✓
Continued infringements of the above, following previous warnings or sanctions.	✓	✓		✓	✓

5. Online Safety Education

5.1 Online Safety Education for Pupils

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

- The school has a planned online safety curriculum for all year groups matched against a nationally agreed framework.
- Lessons are matched to need; are age-related and build on prior learning.
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes.
- Learner needs and progress are addressed through effective planning and assessment.
- The curriculum also incorporates/makes use of relevant national initiatives and opportunities, e.g. Safer Internet Day and Anti-Bullying Week.
- The curriculum is accessible to learners at different ages and abilities, such as those with additional learning needs or those with English as an additional language.
- Regular reference is made to the pupil acceptable use agreement.

5.2 Online Safety Education for Staff

In order to ensure all staff understand their responsibilities as outlined in this policy:

- A planned programme of formal online safety and data protection training is made available to all staff. This is regularly updated and reinforced. An audit of the online safety training needs of all staff is carried out regularly. Records of online safety training are kept and monitored alongside the school's safeguarding training records. Training includes:
 - Online Safety Training (at least annually) based on updated guidance, including the latest Keeping Children Safe in Education guidance and filtering and monitoring expectations.
 - Cyber Security Training (at least annually) based on the latest National Cyber Security Centre guidance.
- The training is an integral part of the school's annual safeguarding and data protection training for all staff.
- All new staff 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 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 are shared with staff, with staff confirming they have read and understand the policy.
- The Designated Safeguarding Lead/Online Safety Lead provides advice / guidance / training to individuals as required.

5.3 Online Safety Education for Governors

Governors receive appropriate online safety training to enable them to effectively carry out their roles. This can take a number of forms:

- Attendance at training provided by the local authority or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

A higher level of training is made available to (at least) the Safeguarding Governor (with responsibility for online safety). This includes:

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

5.4 Online Safety Education for Parents / Carers

The school seeks 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 or via online platforms / newsletters.
- The learners – who are encouraged to pass on to parents the online safety messages they have learned in school.
- Reference to the relevant websites/publications.

6. Technology Infrastructure

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. In carrying out this responsibility, the school has an external service provider to provide expert support.

6.1 Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements, informed by Department for Education (DfE) guidance, Keeping Children Safe in Education, and the Digital and Technology Standards.

- 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 OSL.
- Password policy and procedures are implemented, consistent with guidance from the National Cyber Security Centre (see below).
- There are regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software, managed by the IT service provider.
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud, managed by the IT service provider.
- The SLT, via the IT service provider, 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.
- Users are trained to report any actual / potential technical incident / security breach to the relevant person.
- Use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them.
- Personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network.
- Staff members are not permitted to install software on school-owned devices without the consent of the OSL / IT service provider.
- Removable media is not permitted unless approved by the OSL / IT service provider.

6.2 Filtering and Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors 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.

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider. Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced, e.g. using SWGfL Test Filtering.

6.2.1 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 standards for schools and colleges.

- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.
- The IT service provider, Headteacher and OSL are able to make alterations to the filtered content where there is a clear case to filter content to protect users or unfilter content to enable the appropriate and effective dispensation of school activities.
- Filtering logs are regularly reviewed and alert the DSL and OSL 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).
- The school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

6.2.2 Monitoring

The school has monitoring systems in place to protect the school, systems and users that meets the standards defined in the DfE standards for schools and colleges.

- Monitoring strategies involve both physical monitoring (e.g. adult supervision in the classroom) and digital monitoring (via the RM Safety Net platform).

- The school monitors all network use across all its devices and services. All users are aware that the network (and devices) are monitored.
- Automatic alerts inform the DSL and OSL of breaches to the filtering policy.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the OSL/DSL.
- Alerts that require rapid safeguarding intervention are prioritised, e.g. breaches of illegal content lists trigger an automatic and immediate notification to the OSL and DSL.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

6.3 Password Security

6.3.1 Password Principles

Password policy and procedures are implemented, consistent with guidance from the National Cyber Security Centre.

- School networks and systems are protected by secure passwords. Further or alternative protection is used wherever possible, for example, using Multi-Factor Authentication (MFA) or (Single Sign On) SSO, particularly for accounts with access to sensitive or personal data.
- Security measures are in place to reduce brute-force attacks and common passwords are blocked.
- Passwords are encrypted by the system to prevent theft.
- Passwords do not expire and the use of password managers is encouraged.
- Passwords are immediately changed in the event of a suspected or confirmed compromise.
- No default passwords are in use. All passwords provided “out of the box” are changed to a unique password by the IT Service Provider.
- A copy of administrator passwords is kept in a secure location.
- All users have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords using 3 three random words and with a length of over 12 characters are considered good practice.

6.3.2 Learner Passwords

There is a risk-based approach to the allocation of learner usernames and passwords.

- For younger children and those with special educational needs, learner usernames and passwords can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. Password complexity for these users could be reduced (for example 6-character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.
- Learners are encouraged to set passwords with an increasing level of complexity. Passwords using 3 three random words and with a length of over 12 characters are considered good practice.
- Users will be required to change their password if it is compromised.
- Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

6.4 Mobile Technology

6.4.1 Permitted Mobile Devices

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 <i>personal devices include mobile phones and other devices with similar messaging, photographing or recording features</i>		
	Individual Use	Multiple Users	Pupil Owned	Staff Owned	Visitor Owned
Allowed in School	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> only Y5/6; handed in at start of day and collected at end; not used during school day	<input type="checkbox"/> only for use in the staff room	<input type="checkbox"/> only for use in the staff room
Network Access	<input checked="" type="checkbox"/> full <input type="checkbox"/> guest wi-fi only <input type="checkbox"/> none	<input checked="" type="checkbox"/> full <input type="checkbox"/> guest wi-fi only <input type="checkbox"/> none	<input type="checkbox"/> full <input type="checkbox"/> guest wi-fi only <input checked="" type="checkbox"/> none	<input type="checkbox"/> full <input checked="" type="checkbox"/> guest wi-fi only <input type="checkbox"/> none	<input type="checkbox"/> full <input checked="" type="checkbox"/> guest wi-fi only <input type="checkbox"/> none
	<ul style="list-style-type: none"> are used for the purpose of carrying out school functions where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource there is an asset log that clearly states whom a device has been allocated to liability for damage aligns with current school policy for the replacement of equipment education is in place to support responsible use 		<ul style="list-style-type: none"> personal devices commissioned onto the school network are segregated effectively from school-owned systems by using the guest wi-fi personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school users are responsible for keeping their device up to date through software, security and app updates education about the safe and responsible use of mobile devices is included in the school online safety education programmes 		

6.4.2 Searching, Screening and Confiscation

Members of the SLT have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules. Further guidance is provided in the DfE's [Searching, Screening and Confiscation guidance](#).

- Searching with consent - Authorised staff may search with the learner's consent for any item.

- Searching without consent - Authorised staff may only search without the learner's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for.
- 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 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.
- The person conducting the search may not require the learner to remove any clothing other than outer clothing.
- 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.
- If the member of staff conducting the search suspects they may find an indecent image of a child (sometimes known as nude or semi-nude images), the member of staff should never intentionally view the image, and must never copy, print, share, store or save such images. When an incident might involve an indecent image of a child and/or video, the member of staff should confiscate the device, avoid looking at the device and refer the incident to the designated safeguarding lead (or deputy) as the most appropriate person to advise on the school's response. Handling such reports or concerns can be especially complicated and schools should follow the principles as set out in [Keeping children safe in education](#).
- 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.
 - 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.
 - The responsible person will ensure that full records are kept of incidents involving the searching for and of electronic devices and the deletion of data/files.

7. Social Media

Social media is a broad term for any kind of online platform which enables people to directly interact with each other. The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents / carers and learners are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

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

7.1 Staff Use of Social Media

School staff should ensure that:

- no reference should be made in social media to learners, parents/carers or school staff.
- they do not engage in online discussion on personal matters relating to members of the school community.
- personal opinions should not be attributed to the school.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media.

Personal communications on social media are considered in the following way:

- 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.

Pupils are not allowed to be 'friends' with or make a friend request to any member staff, governor, volunteer and contractor or otherwise communicate via social media. Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, and should be declared upon entry of the pupil or staff member to the school. Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

7.2 School Social Media Accounts

The school holds a social media presence on 'X'. Activity on this account is processed, managed, moderated and monitored by the SLT. Instances of abuse and misuse are responded to in line with this policy and/or utilising guidance from external organisations.

7.3 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. 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.

In the event of any social media issues that the school is unable to resolve support may be sought from the [Professionals Online Safety Helpline](#).

8. Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through a public-facing website and social media (X).

The school website is hosted by Wix and managed by the SLT.

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 – ensuring that there is least risk to members of the school community, through such publications.

Where 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.

9. Digital and Video Images

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

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

- The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies. Guidance can be found on the [SWGfL Safer Remote Learning](#) web pages and in the [DfE Safeguarding and remote education](#) guidance.
- When using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- In accordance with [guidance from the Information Commissioner's Office](#), parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other learners in the digital / video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images. Images/videos should be taken on school devices as far as possible; members of SLT may occasionally use personal devices, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services.
- 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 the 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. Permission is obtained on a child's entry to the school and an updated spreadsheet is maintained with appropriate permissions. Permission is not required for images taken solely for internal purposes.
- Photos are stored on the Priory Education G Drive account in line with the retention schedule of the school Data Protection Policy.

Appendix 1: Loaned Device Indemnity Form

Date

Dear Name of Parent/Carer,

We have provided pupil name with a loan device (e.g. Chromebook) for reason (e.g. home learning).

The DfE's statutory guidance 'Keeping Children Safe in Education' states that schools and colleges in England "should include appropriate filtering and monitoring on school devices and school networks". Please be aware that you will not have this filtering system in place at home therefore, please ensure you are monitoring the content that name of child is accessing at all times.

We would be grateful if you would please sign and return the reply slip below to confirm safe receipt of this device. You are also signing to agree this will be looked after and returned by you as the parent/carer to the School Office in a clean and good working order.

Please advise the School Office of any issues with the device as soon as possible during the loan period.

The device (Make, model no. & serial no.) must be returned by date.

With kind regards,

The Priory School Office

Remote Learning - Loan of Device Reply Slip

I confirm I have received a name of device (Make, model no. & serial no.) on loan from the Priory School for pupil name.

Name: _____








Signed: _____

Date: _____



Appendix 2: Acceptable Use Agreement - EY/KS1 Pupils

Acceptable Use Agreement - EYFS & KS1 Pupils

To keep everyone safe, healthy and happy online:

	<p>I only use devices or apps, sites or games if a trusted adult says so.</p>
	<p>I will take care when using computers and other devices.</p>
	<p>I ask a trusted adult if I am not sure what to do or if I think I have done something wrong.</p>
	<p>I tell a trusted adult if I'm upset, worried, scared or confused, or if I see something that upsets me on the screen.</p>
	<p>I don't keep secrets or do dares and challenges just because someone tells me I have to.</p>
	<p>I always check before sharing personal information.</p>
	<p>I am kind and polite to everyone. I look out for my friends and tell someone if they need help.</p>

I have trusted adults that I can speak to at school and at home.










My Trusted Adult(s) at School	My Trusted Adult(s) at Home
 <p>_____</p>	 <p>_____</p>









My name is _____ and I have read and understood these rules.

Appendix 3: Acceptable Use Agreement - KS2 Pupils

Acceptable Use Agreement - KS2 Pupils



To keep everyone safe, healthy and happy online:

	I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
	I follow age rules.
	I keep my username and password safe and secure and not share it with anyone else.
	I understand new online friends might not be who they say they are – I am careful when someone wants to be my friend. Unless I have met them face-to-face, I can't be sure who they are.
	I am careful what I share and protect my online reputation – I know anything I do can be shared and might stay online forever (even if I delete it).
	I only give out personal information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends.
	I keep my body to myself online – I never get changed or show what's under my clothes when using a device with a camera.
	I check with a trusted adult before I meet an online friend for the first time. I never go alone.
	I ask for help if I am scared or worried – I will talk to a trusted adult if anything upsets me or worries me online.
NO	I don't have to do something just because someone dares or challenges me to do it, or to keep a secret.

	I use and handle devices carefully and only use them if I have permission. I will tell an adult if a device is damaged or if anything else goes wrong.
	I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults.
	I will not try to alter the settings on any devices or try to install any software or programmes.
	I only use text, images or videos from other people if I have their permission.
	I am kind and polite to everyone. I look out for my friends and tell someone if they need help. I won't share or say anything that I know would upset another person or they wouldn't want shared.
	I only take or share images of people if I have their permission.
	I will only bring my personal device (mobile phone or smart watch) to school if I have permission, I am in Year 5 or 6 and I will hand it in to keep it safe.
	When I am using the internet to find information, I will take care to check that the information is accurate, as the work of others may not be truthful and may be a deliberate attempt to mislead me.

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 know that all school devices and systems are monitored, including when I'm using them at home.

I have trusted adults that I can speak to at school and at home.






My Trusted Adult(s) at School	My Trusted Adult(s) at Home
 <p>_____</p>	 <p>_____</p>






My name is _____ and I have read and understood these rules.

Appendix 4: Acceptable Use Agreement - SEND Pupils

Acceptable Use Agreement - Pupils With SEND






   
What I Must do to Keep Safe Online and With Devices

  
Online means anything connected to the internet. Most devices and  
apps are connected to the internet.

  
Devices are technology like: computers, laptops, games consoles,  
tablets and smart phones.

   
I will only use the devices I am allowed to use.

         
I will ask a trusted adult before I use new websites, games or apps.

    
I will ask for help if I'm stuck or not sure.

    
I will be kind and polite to everyone online.

      
I will tell a trusted adult if I feel worried, scared or nervous when I am using a device.



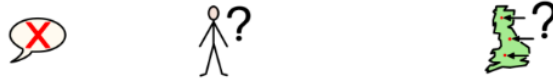
I will tell a trusted adult if I feel sad, angry or embarrassed when I am using a device.



I will tell a trusted adult if I feel bad or unsafe when I am using a device.



I know people online sometimes tell lies.



They might lie about who they are or where they live.



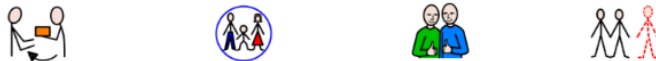
I will always ask a trusted adult before telling anyone my private



information or location.



I know that anything I do or say online might stay there forever.



It can be given to my family, my friends or strangers.



My trusted adults are _____ at school



My trusted adults are _____ at home



My name is _____

Appendix 5: Acceptable Use Agreement - Parents

Acceptable Use Agreement - Parents / Carers

Background

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 agreement 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 pupils have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. Each pupil is asked to agree to an acceptable use agreement - these are available to view in the Online Safety Policy on the school website.

Acceptable Use Agreement

- I understand that the school has discussed the acceptable use agreement with my child 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 child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.
- I will follow the school's position on the use of digital images and video, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.

Appendix 6: Acceptable Use Agreement for Staff

Acceptable Use Agreement - Staff, Governors and Volunteers

Background

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, governors 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, governors 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 Agreement

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 out of school, and to the transfer of personal data out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policy.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, without consent from the SLT or IT consultant.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- 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.

Appendix 7: Acceptable Use Agreement for Visitors

Acceptable Use Agreement - Visitors

Background

This acceptable use agreement is intended to ensure that community users of school digital technologies will be responsible users and stay safe while using these systems and devices; that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk; and that users are protected from potential harm in their use of these systems and devices.

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school through any means, unless I have permission from the school.
- I will not, without permission, 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 school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, whatever the cause.
- 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 if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices.