

# Online Safety Policy

## Introduction

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.

## What is it? Why is it important?

The internet is an essential element in 21<sup>st</sup> century life for education, business and social interaction. At St. John's C of E VC Primary School we believe the school has a duty to provide pupils with quality internet access as part of their learning experience and to empower them to use it safely within, and outside of school. We also have a responsibility to ensure the online safety of staff, volunteers, governors and the wider school community and as such will share good online safety practices and knowledge.

## What do we aim to achieve?

- To provide internet access expressly for educational use and include filtered material content appropriate to pupils, staff, volunteers and governors.
  - Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
  - Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
  - Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
  - To ensure all pupils learn appropriate internet use and be given clear objectives for internet use.
  - To ensure that online safety is learnt throughout the school with each relevant unit of work through our planned curriculum and through PSHE and computing lessons.
  - To ensure all pupils learn how to be critically aware of the content they access online in all lessons and how to validate the accuracy of information.
  - To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
  - To ensure that all pupils are able to use technology to communicate safely and appropriately both inside and outside of school.
  - To ensure that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
  - To ensure pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

## Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, 'Keeping Children Safe in Education', and its advice for schools on:

'Teaching online safety in schools'; 'Preventing and tackling bullying'; 'Cyber-bullying: advice for headteachers and school staff' and 'Searching, screening and confiscation.'

It also refers to the Department's guidance on protecting children from radicalisation with the Counter Terrorism and Securities Act 2015. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

## 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.

### The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

All Governors will:

- Ensure that they have read and understood this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 9).

### The lead online safety governor will:

- attend regular meetings with the Designated Safeguarding Lead and be part of the Online Safety committee.
- regularly receive (collated and anonymised) reports of online safety incidents.
- check that provision outlined in the Online Safety Policy is undertaken.
- ensure that the filtering and monitoring provision is reviewed and recorded, at least annually.
- report to the relevant governor committee.

### The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

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. As DSL, there is also the additional responsibility of day-to-day online safety, as defined in Keeping Children Safe in Education.

The headteacher:

- should, along with the deputy head team, be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- is responsible for ensuring that the Online Safety Lead (OSL), IT provider, 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.
- 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.
- will receive regular monitoring reports from 'Trading with Schools'.
- will work with the responsible Governor, the Online Safety Lead and IT service providers in all aspects of filtering and monitoring.
- provide regular reports on online safety in school to the online safety committee and governing board.

The headteacher as DSL will:

- Hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.
- Meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out.
- Attend relevant governing body meetings/groups.
- Be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- Liaise with staff and IT providers on matters of safety and safeguarding and welfare.

### The Online Safety Lead

The Online Safety Lead (OSL) takes lead responsibility for online safety in school, in particular they will:

- lead the Online Safety Group.

- have a leading role in establishing and reviewing the school online safety policies.
- work closely with the Designated Safeguarding Lead (DSL).
- support the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- work with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments.
- manage all online safety issues and incidents in line with the school child protection policy and ensuring that any online safety incidents are logged (see appendices 5,6,7,8) and dealt with appropriately in line with this policy, by or with, the DSL.
- ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour and anti-bullying policy.
- update and deliver staff training on online safety (appendix 13 contains a self-audit for staff on online safety training needs).
- liaise with other agencies and/or external services if necessary.
- promote an awareness of and commitment to online safety education across the school and beyond.
- liaise with Year Group Leaders (YGLs) to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.
- check filtering and monitoring systems termly to make sure that the system setup has not changed or been deactivated.
- consult stakeholders – including staff/parents/carers about the online safety provision.

This list is not exhaustive.

#### Network Manager/Technical Staff

The network manager and technical staff are responsible for maintaining a safe infrastructure and must be aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively. In line with these policies, they will ensure:

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

### Computing Leads

Computing Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme. This will be provided through:

- Project Evolve.
- PHSE and SRE programmes.
- assemblies and pastoral programmes.
- relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

### Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices.
- they have read, understood and signed the staff acceptable use agreement (AUA) (Appendix: 10).
- they report any online safety issues, and record them on CPOMS. Any online safety issues must be dealt with in accordance with the 'Online Safety Response Grid and Flow Chart' (Appendix: 5, 6, 7) This will be done in conjunction with the headteacher and/or OSL.
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems (See appendix:10).
- they teach online safety lessons and support pupils with online safety matters; seeking advice and guidance where needed.
- pupils understand and follow the Online Safety Policy and acceptable use promises (Appendix:1 & 3).
- they monitor the use of digital technologies, ipads, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches including reporting any filtering issues directly to ICT support, the Head teacher and Online Safety Lead (OSL)
- Where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies (n.b. the guidance contained in the SWGfL Safe Remote Learning Resource).
- 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.

This list is not intended to be exhaustive.

### Volunteers and Visitors

- Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix:11).
- All volunteers and visitors are expected to ensure they tell a member of staff if they see or hear anything that concerns them.

### Parents and Carers

Parents and Carers are responsible for ensuring that they:

- reinforce the online safety messages provided to learners in school.
- notify a member of staff of any concerns or queries regarding this policy.
- ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 2 and 4).
- ensure their child has read, understood and agreed to the terms of bringing a mobile phone to school where this is relevant.
- follow school policy on taking photographs and films during school events (Appendix: 9).
- read the parental consent form when their child starts at St. John's - this includes the acceptable use promise for Computing and guidance for video, sound and images for web publication - and then complete the online google document to show agreement and consent. (See Appendices: 2, 4 & 9).

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

- Taking every opportunity to help parents and carers understand online safety issues through regular guidance in bulletins and on the school website, and inform families about any national/local online safety campaigns/literature.
- Seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA in the appendix).
- Publishing the school Online Safety Policy on the school website.
- Providing them with a copy of the learners' acceptable use agreement.
- Publishing information about appropriate use of social media relating to posts concerning the school.

### Learners

- Are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this should include personal devices – where allowed).
- 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.
- Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience.

### The Online Safety Committee

The Online Safety Committee has the following members:

- Designated Safeguarding Lead & Headteacher.
- Online Safety Lead.
- Senior leaders.
- Online safety governor.
- Teachers.

The Online Safety Committee will:

- contribute to the production/review/monitor the school Online Safety Policy/ documents.
- contribute/review/monitor the school filtering policy and requests for filtering changes.
- Map and review the online safety education provision – ensuring relevance, breadth and progression and coverage.
- Review network/filtering/monitoring/incident logs, where possible.
- Encourage the contribution of learners to staff awareness, emerging trends and the school's online safety provision.
- Monitor improvement actions identified through use of the 360-degree safe self-review tool.
- Filtering and Monitoring.
- 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.
- 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.
- Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader and/or the Designated Safeguarding Lead, in particular when a safeguarding risk is identified or there is a change in working practice.

## 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 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.
- Pupils to report to teacher/trusted school adult.
- Staff to reporting to the IT helpdesk and informing the headteacher plus the online safety lead.
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes (see Appendix for more details).
- Filtering logs are regularly reviewed and the Designated Safeguarding Lead is alerted to breaches of the filtering policy, which are then acted upon.
- The school has provided enhanced/differentiated user-level filtering.
- 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.

## 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 DSL, 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 responses to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

## 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 - Trading with Schools.
- 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 Committee.

- Password policy and procedures are implemented (consistent with guidance from the National Cyber Security Centre).
- The security of their username and password must not allow other users to access the systems using their log on details.
- All users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- All school networks and systems will be protected by secure passwords. Passwords must not be shared with anyone. (see section on passwords in 'Technical security policy template' in the Appendix C1).
- The administrator passwords for school systems are kept in a secure place, e.g. school safe.
- There is a risk-based approach to the allocation of learner usernames and passwords. (see 'Technical security policy template' in the Appendix C1 for more information).
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
- The Business Manager alongside IT support are responsible for ensuring that all software purchased by and used by the school is adequately licenced and IT support are responsible for the latest software updates (patches) being applied.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.
- Use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them.
- Personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network.
- Staff members are not permitted to install software on school-owned devices without the consent of the SLT/IT service provider.
- Staff should avoid using removable media but when necessary a virus scan should be conducted on insertion.
- Systems are in place to control and protect personal data and data is encrypted at rest and in transit. (See school personal data policy template in the appendix for further detail).
- Mobile device security and management procedures are in place.

### Artificial Intelligence (AI)

There are currently three dimensions of AI use in schools; learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible.

- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR.
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools. They must always recognise and safeguard sensitive data.
- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

## Conclusion

We aim to deliver an effective approach to online safety which empowers us to protect and educate pupils, staff, volunteers, governors and the wider school community in its use of technology. We aim to provide an environment in which pupils have access to quality digital resources that enrich their learning experience, give opportunities for productive outcomes and teach children to be responsible and safe users of digital technologies.

- *This should also be read in conjunction with the following policies:*
- *Anti-bullying.*
- *Behaviour.*

- *Safeguarding.*
- *Computing.*
- *PSHE.*
- Bristol City Council Code of Conduct.
- Data Protection.

Due regard was taken by carrying out an EqlA to consider the impact on protected groups. However, the impact of the proposal was positive (or at least neutral) for all.	Tick required: <b>✓</b>	Date: January 2026
--	-------------------------	--------------------

#### Appendix: 1 EYFS & Year 1 & 2 Pupils

### Acceptable Use Promise

**These rules help us to be fair to others and keep everyone safe when we use computers or tablets**

**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/chromebooks
- I will only use activities that a teacher or a trusted adult has told or allowed me to use.
- I will take care of the computer 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.

## Appendix: 2

**Parents/Carers to sign online - EYFS and Years 1 and 2****Acceptable Use Promise**

**These rules help us to be fair to others and keep everyone safe when we use computers or tablets**

**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 the computer 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.

**Parent/Carer's Consent for Internet Access**

I have read and understood the school rules for responsible internet use and give permission for my son/daughter to access the internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed by my child through the internet. I agree that the school is not liable for any damages arising from use of the internet facilities.

**Appendix: 3**    **Years 3-6 Pupils to sign**

## Acceptable Use Promise

**These rules help us to be fair to others and keep everyone safe**

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.

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

- When online, I will act as I expect others to act towards 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:

- If I have permission to bring my mobile phone to school then I must not use it on the school site and hand it in to a teacher as soon as I enter the classroom.
- Other personal devices are not to be used in school without permission from the headteacher.
- I will not access or use social media sites in school.
- 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 disciplinary action. This could include loss of access to the school network/internet, loss of privilege, parents/carers contacted and in the event of illegal activities involvement of the police.

### Learner Acceptable Use Promise Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use promise. If you do not sign and return this promise, 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 use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- 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:

**Appendix: 4      Parents/Carers to sign online - pupils in Years 3-6****Acceptable Use Promise****These rules help us to be fair to others and keep everyone safe**

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.

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

- When online, I will act as I expect others to act towards 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:

- If I have permission to bring my mobile phone to school then I must not use it on the school site and hand it in to a teacher as soon as I enter the classroom.

- Other personal devices are not to be used in school without permission from the headteacher.
- I will not access or use social media sites in school.
- 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 disciplinary action. This could include loss of access to the school network/internet, loss of privilege, parents/carers contacted and in the event of illegal activities involvement of the police.

### Learner Acceptable Use Promise Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use promise. If you do not sign and return this promise, 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 use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

#### **Parent/Carer's Consent for Internet Access**

I have read and understood the school rules for responsible internet use and give permission for my son/daughter to access the internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed by my child through the internet. I agree that the school is not liable for any damages arising from use of the internet facilities.

## Appendix:5

### Response Grid for Dealing with Online Safety Incidents

X = definite action

P = possible action

#### **Pupils**

#### **Actions / Sanctions**

Incidents*: *This includes incidents that happen outside school if they have an impact inside school.	Refer to class teacher	Refer to Head of Year / deputy	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list on unsuitable / inappropriate activities).		X	X	X	X	X	X		X
Unauthorised use of non-educational sites during lessons	X					X if content inappropriate	X (2+ times)	X (1 <sup>st</sup> time)	
Unauthorised use of mobile phone / digital camera / other mobile device	X Handed to office for collection by p/c					X		X (1 <sup>st</sup> )	X (2+ times /term phone withdrawn)
Unauthorised use of social media / messaging apps / personal email	X Handed to office for collection by p/c	P	P			X		X (1 <sup>st</sup> )	X (content dependent)

Status: APPROVED

Version: 1.3

Date Approved: February 2026

Unauthorised downloading or uploading of files	X	X	P			P	P	X (1 <sup>st</sup> )	X (content dependent)
Allowing others to access school network by sharing username and passwords	X	P				P	P	X	
Attempting to access or accessing the school network, using another pupil's account	X	X				P	P	X	
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X	X		X
Deliberately corrupting or destroying the data of other users	X	X	X		X	X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	P			X	P	X	P
Continued infringements of the above, following previous warnings or sanctions	X	X	X	P		X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	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

Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	P		X	X	X	X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	P	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act 2021	X	X					X	X	
Use of AI that is not safe, ethical and or responsible	x	x	x	x	p	p	x	p	p

**Appendix:6****Staff, Governors, Visitors and Volunteers****Actions / Sanctions**

Incidents: * This includes outside school	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning (informal)	Disciplinary action	Suspension
Deliberately accessing or trying to access material that could be considered illegal (see list on unsuitable / inappropriate activities)*.		X	X	X		X	X	
Inappropriate personal use of the internet / social media / personal email	X				X	P	P	
Unauthorised downloading or uploading of files	X			X	X			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X				X			
Careless use of personal data eg holding or transferring data in an insecure manner	X	P			X	P		

Deliberate actions to breach data protection or network security rules		P			X	P		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X			P	P	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	P		X	P	P	
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students / pupils		X	P		X	P	P	
Actions which could compromise the staff member's professional standing	X	P			X	P	P	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		P			X	P	P	
Using proxy sites or other means to subvert the school's filtering system				X	X	P	P	
Accidentally accessing offensive or pornographic material and failing to report the incident				X	X	P		
Deliberately accessing or trying to access offensive or pornographic material		X	X	X		X	X	

Breaching copyright or licensing regulations	X				X			
Continued infringements of the above, following previous warnings or sanctions		P				X	P	
Using AI technologies that are NOT approved by the school	x	x	x			x	x	P
Putting sensitive information in AI technology	x	x	x			x	x	x

## Appendix:7

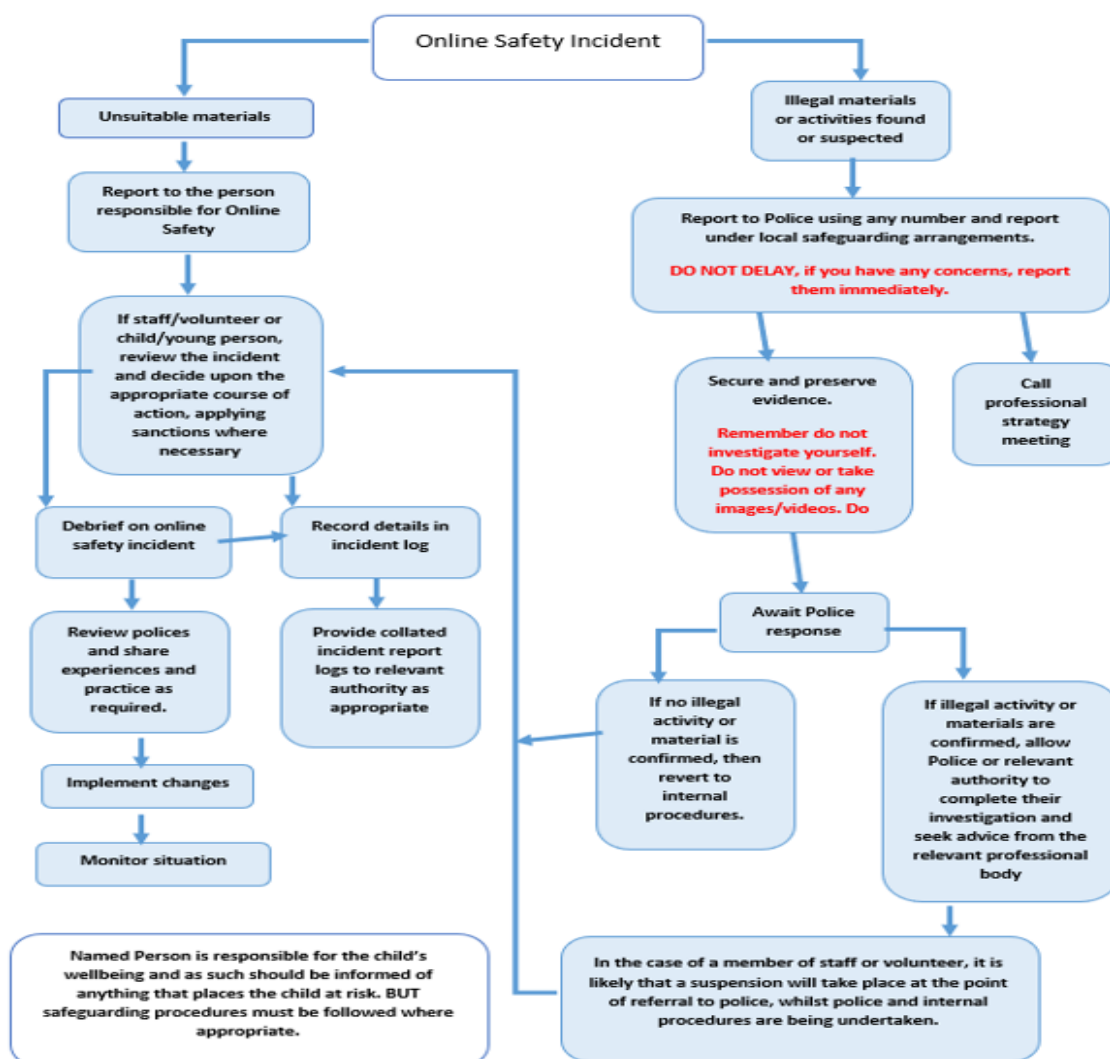
### Dealing with Online Safety Incidents for all members of our school

#### Brief overview of an Online Safety Incident

This would be any action that breaks our **Acceptable Use Promise** (pupils) or **Acceptable Use Agreement** (adults) (See attached sheet). Our list of unsuitable/inappropriate activities gives a clear guide (see attached sheet). It also includes any use of games or websites, including social media sites outside of school, which are not age appropriate, linked to this, any material such as films that are not age appropriate which would be a safeguarding issue.

This should no way be considered an exhaustive guide but used to give an idea of Online Safety Incidents. If at all unsure please talk to Lynda Hood (Online Safety Lead) or Justin Hoye, or Tony Weir (Safeguarding).

#### Responding to incidents of misuse – flow chart



Status: APPROVED

Version: 1.3

Date Approved: February 2026

**Appendix: 8** Form sent digitally with consent given via an online form**Medication - including inhalers and Epipens**

If your child has any medical condition or develops one please inform the school office immediately. We will then ensure a care plan is actioned. ANY MEDICATION brought into school must be prescribed and MUST be signed in. Please bring your medicines to the school office and a member of staff will complete the necessary paperwork. Please allow at least 5-10 minutes for this procedure to be completed.

Please indicate below any illness, allergy or medical problems which we should be aware of.

Your answer

It is necessary for my child to use an inhaler for a medical condition. I will bring a spare prescribed and labelled inhaler, in the original box with instructions, to the school office to be kept in school.\*

Yes

No

It is necessary for my child to have an Epipen. I will bring a spare prescribed and labelled Epipen, in the original box with instructions, to the school office to be kept in school.\*

Yes

No

**Permissions**

In school, photographs are often taken of activities that may involve your child or for use on displays or as a record of achievement. Sometimes photographs may be taken for publication but we need consent in order to do this. Please note that home addresses are never given out to third parties and any photography and filming will only take place with the permission of the headteacher.

I give permission for my child's work, if selected, to be published on the school website.\*

Yes

No

I give permission for photographs that include my child to be published on the school website, subject to the school rule that photographs will not clearly identify individuals by name.\*

Yes

No

I give permission for photographs that include my child to be published externally for example, local publications / marketing literature / newspapers / Local Authority publications, subject to the school rule that photographs will not clearly identify individuals by name.\*

Yes

No

I give permission for my child to take part in visits within walking distance from school. I understand these visits will be well supervised and that they are covered by Bristol City Council school journey insurance. (Details of which are available from the office on request).\*

Yes

No

I give permission for my child to be seen by the School Nursing Team for routine medical examinations or surveys?\*

Yes

No

I/we understand that photographs can only be taken at school performances and events. I/we understand no photographs that show other children / individuals can be shared or uploaded to any social media platform.\*

I understand the rules around photographs at school

I/we agree not to copy, screenshot or photograph images, videos or work from school work platforms and upload onto other online platforms such as social media. \*

I understand the rules regarding sharing of work from school work platforms

## Communication with PTA

For more information about our PTA and how you can get involved, please visit the PTA page on our website. <https://www.stjohnsprimary.org.uk/community/pta/>

Do you agree for your name and email to be shared with the PTA for contact purposes?\*

Yes

No

## **Appendix: 9**

St. John's C of E VC Primary School

*'Together Fly High Like an Eagle'*

### Online Safety Acceptable Use Agreement

Guidance from Swgfl

#### **Staff and Governors**

**This Acceptable Use Policy is intended to ensure:**

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

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

#### **Acceptable Use Policy Agreement**

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

**For my professional and personal safety:**

- I understand that the school will monitor my use of the digital technology systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school digital technology systems (laptops, email, iPads, school website) 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 when children are not present in the room and any personal use is appropriate to view within school.

- I will not disclose my key system 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 ICT 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 from the headteacher to do so and in this case images will be uploaded onto the school network as soon as possible and images will be deleted off the personal device. 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 unless express permission has been granted for this.
- I will not use chat and social networking sites on school equipment.
- When children are in the room staff should not be accessing personal devices
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities such as discussing work on social networking sites or forums.
- I will abide by the guidance set out by Joanne Harker in 'Guidance for safer working practice for adults who work with children and young people' 2009 set out below

**Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.**

**Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between an adult and a child young person outside agreed protocols may lead to**

**disciplinary and/or criminal investigations. This also includes communications through internet based web sites.**

**The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:**

- When I use my mobile devices (iPad / laptops / mobile phones / USB devices etc) 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 ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- As a general rule, I will not use my personal mobile phone in front of a child/children. Any mobile phone use is in a designated child-free space such as the office or the staff room or may be used in the classroom when no children are present.
- 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.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist 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 without gaining permission first from the Computing Leader or Headteacher. When installing apps on the iPad I will use the school agreed system and follow guidance for this. Nor will I try to alter computer settings, unless permission has been granted through our Technical Support provider, the Computing Leader or Headteacher.
- 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 LA Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be placed on an encrypted memory stick or from one secure email address to another or using One Drive. Paper based Protected and Restricted data must only be transported when absolutely necessary and due care must be taken to protect this data.
- I understand that data protection policy requires that any staff or pupil 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.
- AirServer software is only launched when it is needed and closed straight away afterwards. Before launching (and while using the software) any sensitive files should be closed and not opened. Sims should also not be used while the Air Server software is running.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using AI systems in my professional role I will use these responsibly and:

- will only use AI technologies approved by the school.
- will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks.
- will not upload sensitive school-related information into AI systems.
- will take care not to infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing.
- will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being.

**When using the internet 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 digital technology equipment in school, but also applies to my use of school digital technology 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 Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the police.
- I understand I have a duty or care to report any abuse of this policy by others to the Headteacher or Chair of Governors.

**I have read and understand the above and agree to use the school ICT 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/Governor Name

Signed	Date
--------	------

## St. John's C of E VC Primary School

*'Together Fly High Like an Eagle'*

### Online Safety Acceptable Use Agreement

Guidance from Swgfl

#### ***Volunteers and Visitors to school***

**This Acceptable Use Policy is intended to ensure:**

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

The school will try to ensure that where appropriate volunteers and visitors will have access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect volunteers and visitors to agree to be responsible users.

#### **Acceptable Use Policy Agreement**

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

- I understand I am only permitted to use the school's ICT equipment when under the direct supervision of the class teacher.
- I understand I will only use the ICT equipment as directed by the class teacher.
- I will immediately report any damage or faults involving equipment or software, however this may have happened, to the class teacher.
- 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 understand that I am not permitted to download any material onto the school network. Nor change any of the settings.
- If I have been given permission by the Headteacher or Senior Leadership team for use of personal mobile devices (iPads / laptops / mobile phones / USB devices etc) 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 ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not try to upload, download or access any materials on any device (including personal devices) which are illegal (child sexual abuse images, criminally racist 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 understand that, in conjunction with the confidentiality agreement, I must not share information about the children or school with others and this includes the use of online forums.
- I will not communicate electronically with pupils outside of school.
- **Mobile phones must be put away and on silent mode when working in school. If you have to use your mobile phone then this must take place in an area where no children are present. The phone must not be used to take photographs without permission.**
- I understand I have a duty or care to report any abuse of this policy by others to the Headteacher or Chair of Governors.
- I will abide by the guidance set out by Joanne Harker in 'Guidance for safer working practice for adults who work with children and young people' 2009 set out below

**Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.**

**Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between an adult and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet-based web sites.**

**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 ICT equipment in school, but also applies to my use of personal equipment on the premises or in situations related to my working with the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, termination of our acceptance of you as a volunteer, referral to or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT 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.

Volunteer/Visitor Name:

Signed	Date
--------	------



## Appendix 12 from Online Safety Policy Templates

### Online Safety Committee

#### Terms of Reference

##### 1. Purpose

To provide a consultative group that has wide representation from the school's community, with responsibility for issues regarding online safety and the monitoring of the online safety policy including the impact of initiatives. The Headteacher will also be responsible for regular reporting to the Full Governing Body.

##### 2. Membership

2.1. The online safety committee will seek to include representation from all stakeholders. The composition of the group should include:

- SLT member/s.
- DSL.
- Support staff member.
- Online safety lead.
- Governor.
- Parent/Carer.
- ICT Technical Support staff (where possible).
- Community users (where appropriate).
- Learner representation – for advice and feedback. Learner voice is essential in the make-up of the online safety group, but learners would only be expected to take part in committee meetings where deemed relevant.

2.2. 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.

##### Committee Members:

- Must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.
- Must be aware that many issues discussed by this group could be of a sensitive or confidential nature.
- 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 invitations to meetings.
- 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 meeting notes are taken, with action points and distributed as necessary.

#### **4. Duration of Meetings**

- Meetings shall be held termly for a period of up to 30 minutes. A special or extraordinary meeting may be called when and if deemed necessary.

#### **5. Functions**

The Online Safety Committee will:

- contribute to the production/review/monitor the school Online Safety Policy/documents.
- contribute/review/monitor the school filtering policy and requests for filtering changes.
- Map and review the online safety education provision – ensuring relevance, breadth and progression and coverage.
- Review network/filtering/monitoring/incident logs, where possible.
- Encourage the contribution of learners to staff awareness, emerging trends and the school's online safety provision.
- Monitor improvement actions identified through use of the 360-degree safe self-review tool.

#### **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 St. John's Primary School have been agreed by the headteacher:

Signed by Justin Hoye:

Date:

Date for review: