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 21st 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.

Status: APPROVED

Version: 1.2

Date Approved: July 2024

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 (YGL's)leaders 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
- Publish 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.

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 EqIA to consider the impact on protected groups. However, the impact of the proposal was positive (or at least neutral) for all.	Tick required:√	Date: June 2024

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.