St.John's
CofE Primary School
Clifton & Redland

Online Safety Policy

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.
- 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 and cyber-bullying: advice for headteachers and school staff Searching, screening and confiscation.'

It also refers to the Department's guidance on protecting children from radicalisation. 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

The governing board

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

The governing board will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All Governors will:

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

The Headteacher

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

- Providing regular reports on online safety in school to the online safety committee and governing board

The Online Safety Lead

The Online Safety Lead takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- 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.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 13 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary

This list is not exhaustive.

Network Manager/Technical Staff

Are responsible for :

- Ensuring that the school technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis

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)
- All members of the school are responsible for reporting any online safety issues, and recording them on CPOMS. Staff will also be asked at each staff meeting if there are any online safety issues to be discussed. The Headteacher will keep a record of any online safety issues and deal with accordingly following the 'Online Safety Response Grid and Flow Chart' (Appendix: 5, 6, 7) This will be done in conjunction with the Online Safety Lead Teacher and/or the Online Safety Lead Governor.
- All digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems. See appendix:10
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Online Safety Policy and acceptable use promises Appendix:1 & 3
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, 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

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

Are responsible for ensuring that they:

- Notify a member of staff or the headteacher 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 photograph and films during school events (Appendix:9)

- When children start at St. John's, parents/carers will receive digitally the parental consent form which includes the acceptable use promise for Computing and guidance for video, sound and images for web publication. Every parent must complete an online google document to show agreement and consent. (See Appendices: 2, 4 & 9).

School will support parents by:

- Taking every opportunity to help parents understand online safety issues through regular guidance in bulletins and on the school website and inform parents about any national/local online safety campaigns/literature.

- *Use photographs and videos as agreed Appendix 9*

Pupils

Pupils will be expected to:

- read, understand and agree to the terms on acceptable use of the school's ICT systems and internet for use in school and on home-learning platforms (appendices 1 and 3)
- read, understand and agree to the terms of bringing a mobile phone to school where this is relevant

- keep passwords and QR code logins safe and private

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.

School will ensure:

- We provide a planned online safety curriculum as part of Computing/PHSE/other lessons that is regularly revisited
- We provide key online safety messages that are reinforced as part of a planned programme of assemblies and other activities
- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will be 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.

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

COVID- 19 – Interim Safeguarding Guidance Addendum to the Safeguarding/Child Protection Policy

Bristol City Council Code of Conduct

GDPR

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
- 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 am unsure about something I have done on the computer.
- 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.

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

- 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.

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

- I will use devices/computers as my teacher has asked, only accessing the programs or applications they have asked me to use.
- I will ask permission before using the internet.
- I will use only my own or year group network login and password, which is secret.
- I will only open or delete my own files.
- I understand that I must not bring into school and use software or files or personal devices without permission.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will only e-mail, open attachments or download a file from people I know and trust, or my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my full name, home address or phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or friends, unless a trusted adult has given permission.
- I must have parental permission to meet someone in person that I have only ever previously met on the Internet.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files, e-mails I send and the internet sites I visit.
- I should ensure that I have permission to use the original work of others in my own work
- I will not copy, screenshot or photograph images, videos or work and upload onto online platforms such as social media.
- I understand that if I deliberately break these rules there will be appropriate sanctions.

Class: ___________ *Date:* _____________

Signed (all children in class to sign as part of class charter)

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

- I will use devices/computers as my teacher has asked, only accessing the programs or applications they have asked me to use.
- I will ask permission before using the internet.
- I will use only my own or year group network login and password, which is secret.
- I will only open or delete my own files.
- I understand that I must not bring into school and use software or files or personal devices without permission.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will only e-mail, open attachments or download a file from people I know and trust, or my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my full name, home address or phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or friends, unless a trusted adult has given permission.
- I must have parental permission to meet someone in person that I have only ever previously met on the Internet.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files, e-mails I send and the internet sites I visit.
- I should ensure that I have permission to use the original work of others in my own work
- I will not copy, screenshot or photograph images, videos or work and upload onto online platforms such as social media.
- I understand that if I deliberately break these rules there will be appropriate sanctions.

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

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	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X				P		X	
Unauthorised use of social media / messaging apps / personal email	X	X	P			X	P	X	
Unauthorised downloading or uploading of files	X	X	P			P	P	X	
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
Corrupting or destroying the data of other users	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			X	X	X	X
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
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		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	X	X					X	X	

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	X
Inappropriate personal use of the internet / social media / personal email	X	X				X	P	P
Unauthorised downloading or uploading of files	X	P			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	P				X		
Careless use of personal data eg holding or transferring data in an insecure manner	X	P	P			X	P	
Deliberate actions to breach data protection or network security rules		X	P			X	P	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X			P	P
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	P		X	P	P
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students / pupils		X	X	P		X	P	P

Actions which could compromise the staff member’s professional standing	X	X	P			X	P	P
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	P			X	P	P
Using proxy sites or other means to subvert the school’s filtering system		X			X	X	P	P
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X	X	P	
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X		X	X
Breaching copyright or licensing regulations	X	P				X		
Continued infringements of the above, following previous warnings or sanctions		X	P				X	P

Appendix:7

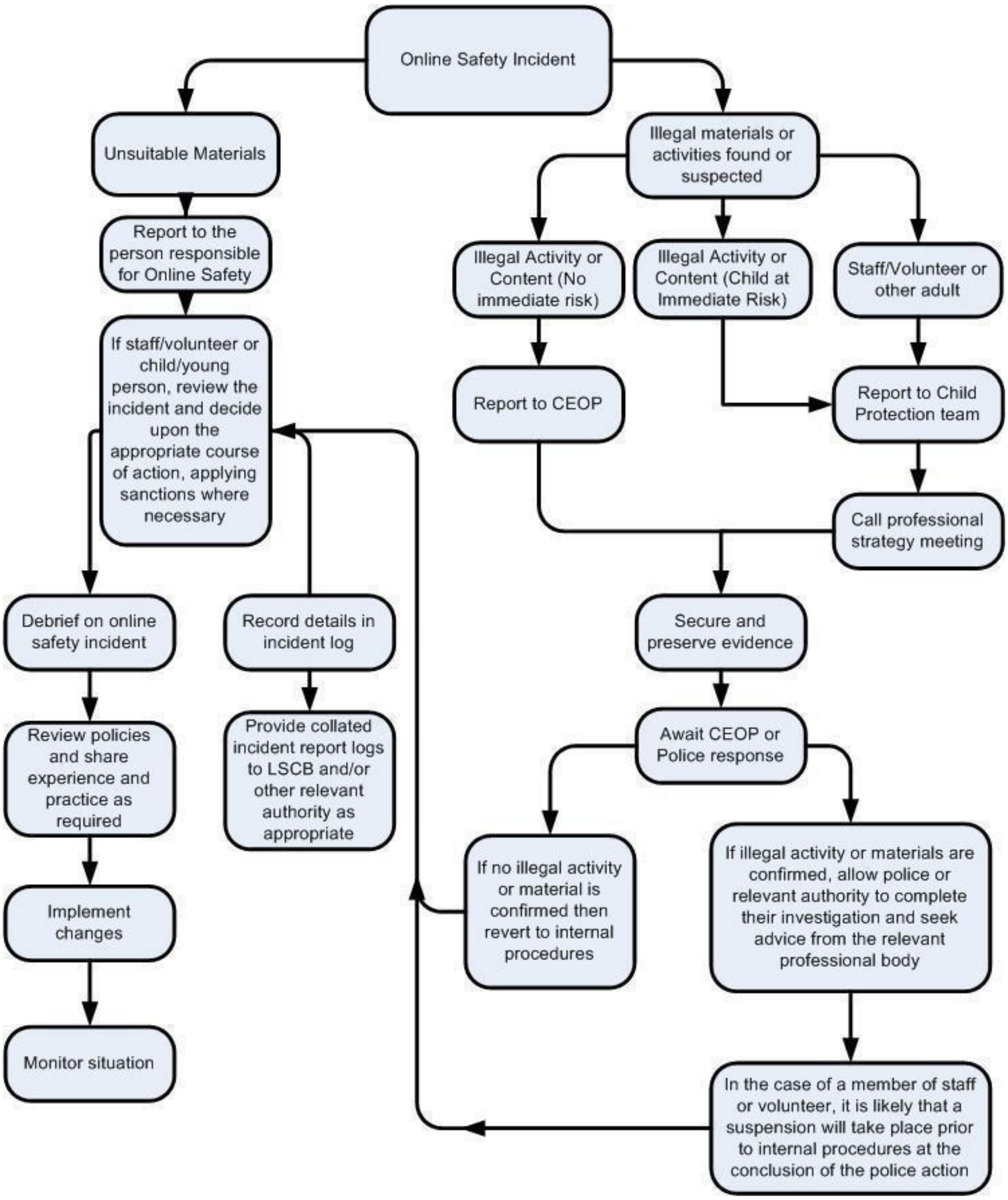
Dealing with Online Safety Incidents for all members of our school

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, Ali Vining or Tony Weir (Safeguarding).

Responding to incidents of misuse – flow chart


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Appendix: 8 Reporting Log

Reporting Log

Group: ______________________________

Date	**Time**	**Incident**	**Action Taken**		**Incident Reported By**	**Signature**
			What?	**By Whom?**		

Appendix: 8 Form sent digitally with consent given via an online form

Name of child .... Class .... Date ....

Short visits within walking distance from the school

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 insurance cover are available from the office on request).

Use of Inhalers

It is necessary for my child to use an inhaler for a medical condition. □

I enclose a spare labelled inhaler in the original box including instructions and prescription label □

Please note that children should be able to administer their own inhaler. It is **essential** that children's inhalers are labelled with their name and class and that a spare is retained in school in case of emergencies. We will notify you if and when the spare inhaler is used so that you can replace it.

Medication

If your child develops any medical condition during the year please inform Mrs Cross immediately. She will then ensure a care plan is actioned. **ANY MEDICATION** brought into school, either prescribed or bought over the counter **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.

Publication of photographs and/or pupils work

In school, photographs are often taken of activities that may involve your child for use on displays or as a record of their 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/we agree, if selected, my son/daughter's work may be published on the school Website. □

I/we agree, if selected, my son/daughter's photograph may be published in the Local Authority

and a local newspaper with their name. □

I/we agree that photographs that include my son/daughter may be published on the school Website subject to the school rule that photographs will not clearly identify individuals and that full names will not be used. □

I/we agree that I/we will only take photographs or videos in school at school events or performances and that if any of these contain images of other children, they will not be uploaded to the internet (including Facebook). □

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. □

Communication Details

I/we agree to allow school to use our mobile phone numbers to contact us via text. □

I/we would like to be included on the class e-mail list so that we can be kept informed of the latest news. (Please ensure email addresses are written **clearly** as this could affect the online payment system) □

My/our e-mail address(es) is:……………………………………………………………………………(**please write clearly)**

□ Tick if you do **NOT** wish this e-mail address to be shared with the other parents of children in your child's class.

□ Tick if you do **NOT** wish this e-mail to be used by PTA Class Reps to remind you of upcoming events.

Signed………………………………………………. Parent/Guardian

Date ……………………………………………

I agree that my responses will be accepted throughout my child's time at St John's UNLESS I inform you otherwise in writing

Signed ……………………………Parent/Guardian Date……………

<u>Appendix: 9</u>

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 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 will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff 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. 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.

For my professional and personal safety:

- I understand that the school can monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (laptops, email, ipads, school website) out of school, and to the transfer of personal data (digital or paper based) out of school.
- Mobile phones should be kept on silent during the school day. In EYFS phones need to be switched off during the school day or kept in the school office. Phones and other personal devices may be used during the school day for work purposes however if required for personal use then must be used in the staff room or off site.
- I understand that the school ICT 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 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 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 in school.

- When children are in the room 'i message' links to iPhones should be switched off on personal and school allocated iPads.

- 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.

- 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 co-ordinator 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 coordinator 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 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 ICT equipment in school, but also applies to my use of school ICT 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

Appendix:10

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 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 working in EYFS then phones must be switched off.   If you have to use your mobile phone then this must take place in the staff room or school office. The phone must not be used to take photographs of the children.
- I understand I have a duty or care to report any abuse of this policy by others to the Head Teacher or Head 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

Appendix11: Guidance given during school lockdown

Guidance for Staff

In this document, we have tried to put together all the relevant information in the event of another lockdown. Please use the links below (press Ctrl) to guide you to the relevant section of the document:

Initial Ways of Working

If we need to switch to remote learning, our plan is to use Seesaw (infants) and Google Classroom (GC) (Juniors) as a platform for providing learning, but accepting that it can never be the same. We will provide 4 English and 4 Maths 'lessons' per week with at least 4 short video inputs over the week. It is up to teams to determine when these would be most effective to aid learning. For the infants the video will be by the class teacher (or partner teacher if you're in school) to reflect the age and nature of the children. In the Juniors, the video may be done by someone else in the team to reflect the age of the children, their independence and the greater digital interaction & feedback required for this age group. It is likely that the majority of videos will be done using Screencasting – this is where the children can see your screen and what you do on it AND hear you verbally or (in a smaller window) see you talking them through it, details below but see this overview: https://youtu.be/uuJ2lF9RkgE

We will then have curriculum learning activities each week – generally 2 'musts' and 4 'coulds' for children to complete. Friday will effectively be a catch-up day for everyone.

Please read and follow the principles and advice below:

1) Teams will aim to have their PPA time together remotely to organise planning, resourcing etc.
2) If you are on the rota to be in school, there is no expectation to plan & resource work. Please do ensure you are released for your PPA though.
3) Children in school will do the same as those at home so they can keep pace with everyone else – many are also dipping in and out of school and home learning so we need to be consistent.
4) Plan screen-based and non-screen-based activities to achieve a healthy screen time balance.
5) Plan carefully for those who cannot access the online platform but be careful not to double teachers' workload – if it can be part of a pack then the office can send this home.
6) Please read the Online Safety advice below for videoing.
7) Activities/videos etc. can be prepared in advance and scheduled to only be 'released' on a particular day – your YGL will organise folders etc. to reflect this.
8) It will be lovely for the children to see your face at the start and end of the video, but research says that it can be a distraction during modelling so do toggle the webcam on and off (easy to do – see Reg's guidance below) – children will still hear your voice. As a rule of thumb, consider what you would do in the classroom i.e. if you were reading a story then you'd want the children to look at you, if you were showing a Smart screen you'd want them to be looking at that.

9) In the first week, LRR will build up to using Seesaw and videos gradually. WR are already using GC, but in week 1 you may want to use straight forward video while you get used to Screencastify. It will be useful for all year groups from week 2 onwards.
10) Don't re-invent the wheel – there is a lot of good stuff out there so feel free to provide links to other resources and activities. But equally, if it's not right then it may be more efficient to come up with something yourself rather than waste time trawling.
11) Think about self-marking – can you provide the answers (especially maths)? This could be on the day on the basis of trust (as many of you do in lessons) or could be released the following day. Feedback could be a recorded verbal message or a screencast could be very effective and less time consuming that writing. Bear in mind our feedback policy of what has the most impact – remember the impact = time input vs learning outcome!
12) Plan your time so it works for you – there is a real danger that you spend all your time worrying about being online and responding to children: Don't! You may want to dip in and out over the school day or you might want to block your time online when it fits with you (or when your spouse can have the kids!). Do what works but build in time for yourself and switching off . . . this may be a long haul.
13) Video shout-outs or posts on the GC Stream to your class are always nice, you may want to highlight particularly good effort/pieces of work but just keep track as some children may be desperate for one and not get it.

14) Many children need a lot of guidance when working and cannot be left for long periods of time to complete complex tasks – aim for activities that children can complete on their own. We must recognise that many parents are also trying to work from home, and parents might struggle to assist with schoolwork for a number of reasons. Parents cannot be expected to become teachers.

Screencasting

This is the ability to record a video of anything that is on your screen, while simultaneously recording your voice and where appropriate showing your face via webcam. We will do this on the school chrome books as they are not personal; have a webcam and mic; are new so reliable; have a stylus so you can write/annotate etc. with ease. Justin or another member of SLT will deliver a chrome book to your house some time in the next week (we will also deliver learning journals to help with report writing).

There is a lot of additional guidance online and it is very intuitive, but Reg has used a Screencast video to teach you how to use screencasting. Hopefully this should give you all the information you need but if you have any problems then Reg is happy to be contacted or you can contact Justin. Please click on this link below:

https://drive.google.com/file/d/1gadN3OMqB66uEype7fJjBgoolcbS5o0P/view?usp=sharing

At the moment, we are able to get the Premium version for free. Reg describes this in the video, but it can be a bit tricky so he has put together some screenshots here which make it really clear:

https://docs.google.com/document/d/13Y_5YvtauCTRdz27YXWJ43qjpEvJ6WL0Kw5cSkXi7Lk

Appendix: 13

Training Needs Audit Log

Group: ______________________________

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date