St. John's Primary School



Online Safety Policy

"Everyone who works with children should do what is in the best interests of the child."

Thinking learning Caring

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- ✓ Websites
- ✓ Email and Instant Messaging
- ✓ Chat Rooms and Social Networking
- ✓ Blogs
- ✓ Podcasting
- ✓ Video Broadcasting
- ✓ Downloading from the internet
- ✓ Gaming
- ✓ Mobile/Smart phones with text, video and/or web functionality
- ✓ Other mobile devices with web functionality

At St John's School, we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. We foster an 'encourage' culture where children discuss online safety issues openly, recognise concerns and feel able to share these with a trusted adult.

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.

"To ignore e-safety issues when implementing the requirements of Every Child Matters could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable."

Safeguarding Children in a Digital World. BECTA 2006

United Nation's Convention on the Rights of the Child (UNCRC)

As a Rights Respecting School our philosophy is underpinned by the values and principles of the United Nation's Convention on the Rights of the Child (UNCRC).

Article 2: All children have these rights and should not be discriminated against.

Article 3: Everyone who works with children should do what is best for each child.

Article 6: Children have the right to survive and develop and should grow up in conditions that don't impact negatively on their physical and mental wellbeing.

Article 12: Children have the right to be listened to and taken seriously.

Article 17: Children have the right to get information in lots of ways, so long as it is safe.

Article 19: Children should not be harmed and should be looked after and kept safe.

Article 28: Children have the right to an education.

Article 29: A child or young person's education should help their mind, body and talents to be the best they can be and should help build respect for other people and the world around them.

Article 36: Children should be protected from doing things that could harm you.

Online Risks

The internet and constantly evolving technology have changed the way that children interact with the world. While this can offer opportunities to learn and express their creativity, this technology also offers news risks such as:

- ✓ Exposure to inappropriate material (either accidentally or deliberately)
- ✓ Cyber bullying
- ✓ Self-Harm
- ✓ Exposure to online predators
- ✓ Sexting
- ✓ Trolling
- ✓ Revealing too much personal information
- ✓ Radicalisation

Learning to recognise warning signs will allow trusted adults to intervene where appropriate and to lessen the impact of potential negative experiences. It is vital for **ALL STAFF** to stay well informed about the issues relating to what children are experiencing using social networking, webcams, blogs, instant messaging etc.

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Headteacher has ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Online Safety Officer in our school is **Miss Georgie Clavel**, the deputy is **Mr Jamie Hazley.** All members of the school community have been made aware of who holds this post. It is the role of the Online Safety Officer to keep abreast of current issues and guidance through organisations such as CEOP. The Online Safety Officer updates the Senior Leadership Team. The SLT understands the issues at our school in relation to local and national guidelines and advice.

Headteacher and SLT

- ✓ The Headteacher and SLT are responsible for ensuring that the e-safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

- ✓ The Headteacher and SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- ✓ The Headteacher is aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- ✓ Reviews the Impero Dashboard Daily to monitor online activity of children.
- ✓ Receives daily reports of e-safety incidents (lightspeed reports) and creates a log of incidents to inform future e-safety developments.
- ✓ Convey clear messages to all staff and students connecting to 3G and 4G networks and unsecured domestic Wi-Fi networks, that this will bypass safeguarding filters in place when using them.

The Online Safety Officer

- ✓ Ensures that children are educated about online safety and related issues.
- ✓ Manage and maintain different user profiles for web filtering to ensure all children are protected to an appropriate level.
- ✓ Manage requests to the Department's Helpdesk, being highly aware of online safety and data protection issues.
- ✓ Escalates safeguarding concerns where appropriate if there are safeguarding concerns, within the school and to the CYPES Department and other agencies such as Child and Family Hub where appropriate.
- ✓ Monitor the selection of web based services chosen by staff and be responsible for approving and completing Data Protection and Impact Assessments (DPIAs) assessing the use of any web based applications that staff wish to use. Challenge choices where appropriate.
- ✓ Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy/documents.
- ✓ Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- ✓ Provides training and advice for staff.
- ✓ Liaises with school Computing Technician- **Mr Tom Dorey.**
- ✓ Monitor and promote positive online safety, through the use of *Lightspeed reports (ceased July 2021)* and currently through the Impero Package.
- ✓ Monitor the school's online profiles and reputation, including on unofficial sites.

All School Staff

- ✓ Monitor and promote positive online safety
- ✓ Act on and escalate all online safety issues promptly and escalate to the Online Safety Officer in accordance with the Child Protection and other Safeguarding policies
- ✓ Sign an Acceptable User Agreement and adhere to the responsibilities set out therein **(See Appendix 3 for copies of both the staff and children's AUP)**
- ✓ Only use work email address to communicate with children (not personal email)

- ✓ If working remotely from home: do not divulge the password to any family members or let any member of the household use the login, laptop or device for any purpose whatsoever; use a designated room or space to work from; keep the device locked up and secure at all times
- ✓ Use every appropriate opportunity to link online safety into the everyday curriculum
- ✓ Encrypt personal information/ special category information (previously referred to as sensitive data) is encrypted or password protected, especially if transferring information. The device information is transferred on should also be password protected.
- ✓ Only use websites and web-based applications with students when they have had a Data Protection and Impact Assessment (DPIA) completed and you have read and reviewed the terms and conditions and are satisfied that they do not pose a significant online safety or data protection risk
- ✓ Not allow anyone else (whether children or other members of staff) to use their log on details or leave their computer or device unattended when logged into
- ✓ Not attempt to compromise or bypass online safety measures for the sake of expedience or convenience
- ✓ Be aware of content which should be blocked (e.g. inappropriate) and report this to The Online Safety Officer/ Deputy promptly if it is not.

Internet Filtering and Blocking

Light speed

St John has internet content filtered centrally by the CYPES Department. This will remove the majority of undesirable content, but it is important to bear in mind that no filtering system is infallible, and some unpleasant content will inevitably sometimes get through. This is particularly true of image searches, where some unpleasant images are tagged with innocuous words.

As a result, all staff must ensure sufficient supervision is in place, and that as a school we develop a culture where children feel they can approach staff if they have seen anything which worries them.

Both the Headteacher and Online Safety Officer receive daily Lightspeed reports and when there is a concerning search these are dealt with according to policy and actions taken are recorded onto the tracking grid saved in the admin shared drive. *False Positives* were not recorded.

Q:\Health and Safety\Suspicious Searches

Staff accounts have much less filtering applied than student accounts. Staff can apply for sites to be unblocked to staff accounts via the school technician when a risk assessment has been completed.

Many digital 'apps' are able to circumvent the central monitoring and filtering so vigilant monitoring of this will be undertaken.

Impero

The Impero System is installed on all staff and student computers and ipads. It is much a much more granular classroom management tool and allows us to see inside draft emails, and word documents. In the UK, internal school technical monitoring is a legal requirement.

The nature of this level of technical monitoring software is that there will be many 'false positives' (such as 'Moby Dick'). However, it is very important that we do not dismiss all of the flags on this basis, as some will be genuine.

Our Online Safety Officer checks our Impero database daily and responds swiftly to the email flags. They log on to review the dashboard; reviews each category by viewing the identified captures; applies a status to each and then takes appropriate action or assigns a false positive status. Should any concern also raise safeguarding concerns this will also be logged onto MyConcern and the suspicious search tracking grid.

See the **Acceptable User Policy** for guidance in acceptable use of technology in school.

Web histories

For children

For safeguarding reasons, the Online Safety Officer is able to request the web history of a child. She will request as a Helpdesk ticket - but will not name the child in the ticket and ask for a call back. The search and the reasons for the report should be documented in the child's file, and the outcome of the report integrated within any other child protection procedures.

For staff

On some occasions it will be legitimate to carry out a web history search for a member of staff. This maybe a formal request as part of a disciplinary procedure or similar. All requests should be from the Head teacher, the Police or to complete a statutory function.

If illegal content is found

If illegal or potentially illegal content is found on the schools' network or a school owned device, the machine is immediately closed down, the room or area will be secured and the advice of the Headteacher will be sought immediately. The Headteacher will then contact the Head of Governance or Head of Inclusion at the CYPES Department who will provide further advice and facilitate contact with the Police.

Do not forward, copy, print or save what you have found as this could potentially be a criminal act (i.e. making indecent images) and lead to a prosecution. The police will review the material and take appropriate action.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- ✓ The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- ✓ Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- ✓ Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- ✓ As part of the new Computing curriculum, all year groups have digital literacy objectives that focus on different elements of staying safe online. These units include topics from how to use a search engine, digital footprints and cyber bullying.
- ✓ The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Through computing, we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society. Each class will ensure that they cover several different strands of Online Safety every term and will take part in Safer Internet Day each year.

Through the use of the school website, parents are able to access resources that will help to support them at home by understanding the different applications and programs that their children access at home. These documents can be found at:

https://www.stjohn.sch.je/page/?title=Online+Safety&pid=21

Children's use of Social Media

At St John's we recognise social media as a particular risk area for children. Unlike in recent years, where young people would be on one platform, young people use a wide variety of online platforms to share personal content. This can mean that any risk and issues are more complex.

Age restrictions. Under U.S. Law a child must be minimum age 13 to use social media platform and this message is shared with the children and parents of the school in newsletters and advice is available on the school website. Under the Data Protection 2018 Legislation, the Information Society has been introduced; this includes when offering an online service directly to a child, in the UK only children aged 13 or over are able provide their own consent.

Bear this in mind when asking children to use social media as part of their learning. Below are the age restrictions for the most common sites:

13: Twitter, Facebook, Instagram, Pinterest, Google+, Tumblr, Reddit, Snapchat, Secret

14: LinkedIn

16: WhatsApp 17: Vine, Tinder

18: Path 18 (but 13 with parent's consent): YouTube, Keek, Foursquare, WeChat, Kik, Flickr

Staff's Social Media accounts

All staff are asked to ensure that their personal Social media profiles are locked down and not publicly viewable.

Staff will not 'friend' or accept friend requests from students on their personal social media profiles- even after they have left school.

If parents or members of the community post negative comments about the school or staff students in the school, we DO NOT respond. Staff know to escalate this information to either Mr Hazley or Mr Pallant who will then seek advice from the Head of Governance at the Department.

Published content on the school web site and social media pages run by the school including images

Permission

Written permission from parents or carers is obtained before photographs of pupils are published on the school Website. This information is stored securely on the admin drive. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue. Parents have a right to change their mind and that decision must be recorded. **(See Appendix 2- Parental Consent Form).** If one parent gives consent and the other does not, you should proceed as if no consent has been given. N.B. you must have legal parental responsibility to give consent.

Parents/carers may withdraw permission, in writing, at any time.

Images of children

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

Pupils' full names will not be used anywhere on the school website, particularly in association with photographs.

If there is a 'one off' reason to publish a child's picture (e.g. a specific event) then the school will contact the parents to seek specific consent for that event. Once the press image has been captured with consent, the media organisation is then the data controller for that image.

Parents and carers can take pictures of their own children at their school provided it is for their own personal use and not uploaded to social networking sites.

Staff / volunteers can take pictures to support educational aims, but must follow school policies regarding the sharing, distribution and publication of those images.

The images should only be recorded on school owned devices, not personal devices. Care should be taken that students are appropriately dressed and are not participating in activities that might bring the school into disrepute.

Students must not take/use/share pictures of other students without permission.

Photographs published on the school website or elsewhere on behalf of the school will be selected carefully and appropriate consent sought.

Where consent has ben gained, the school must not provide more than two pieces of identifiable data (e.g. school uniform and their first name would be two pieces of data). Children's names should not be shared on the school's social media page.

Use of mobile devices

Children in year 4, 5 and 6 who walk to school are allowed to bring their mobile phones to school with them. This can help parents with peace of mind regarding their safety.

Mobile devices accessing the internet via 3G, 4G or unsecured domestic Wi-Fi networks are not subject to the same filtering and monitoring that the school systems are. Staff are aware that this could potentially give access to unsuitable content whilst on school grounds to the owner of the device and their peers. Whilst under school supervision, children are asked to hand the phone into the school office to look after for the day. These are stored in a safe place.

No member of the school community (staff, volunteers and pupils) should use their mobile phone to call, text or go online, when working with the children. Phones should be used in the staffroom or in appropriate areas where reception can be gained.

If there is any concern that there have been e-safety issues arising from the use of mobile devices, the Online Safety Officer should be made aware and will seek guidance from the Head of Compliance- **Mrs Alexa Munn.**

Key questions addressed by the Online Safety Officer to ensure online safety compliance

- ✓ Are you writing new and updated polices and distributing them?
- ✓ Are you involving all of your staff in online safety and training them where appropriate? DO all staff see online safety as their responsibility?
- ✓ Are you making use of filtering and monitoring software?

- ✓ Are you engaging parents, carers and the wider community?
- ✓ Are you maintaining accurate records of online safety incidents and including them on the child's file?

- ✓ Do the children in your school understand the risks around online safety and how to respond if they see anything that worries them?

CHANGE HISTORY

Version	Date Issued	Issued by	Reason for Change	Presented To	Approved by:	Date
0.1	October 2022	Georgie Clavel	Draft in line with CYPES Online Safety Policy (August 2021)	Teaching staff	J. Hazley	

Appendix 1- Further Departmental Information around Online Risks

Cyber-Bullying

Bullying is behaviour that is deliberate, repeated more than once and is designed to be hurtful. This type of behaviour can happen both on and offline (and often both), so it is crucial to consider all surrounding behaviour.

The impact of online bullying. While cyber-bullying can be an extension of face-to-face bullying, it differs in several significant ways: the invasion of home and personal space; the difficulty in controlling the scale and scope electronically circulated messages; the size of the audience; perceived anonymity; and even the profile of the person doing the bullying and their target is often different to 'offline' bullying.

Policies and signposts for reporting. Schools must have anti-bullying policies which articulate that participating in such activity will not be tolerated and provide clear guidance as to who a child should contact if they feel that they or someone else is being bullied.

Support for the target. The target of cyberbullying may be in need of emotional support. Key principles here include reassuring them that they have done the right thing by telling someone; recognising that it must have been difficult for them to deal with; and reiterating that no-one has a right to do that to them. Refer to any existing pastoral support/procedures for supporting those who have been bullied in the school and refer them to helpful information and resources.

Advice for the target. It is important to advise the person being bullied not to retaliate or return the message. Replying to messages, particularly in anger, is probably just what the bully wants, and by not replying the bully may think that the target did not receive or see the message, or that they were not bothered by it. Instead, the person should keep the evidence and take it to their parent, or a member of staff Advise the pupil to think about the information they have in the public domain and where they go online. Advising the child to change their contact details, such as their Instant Messenger identity or mobile phone number, can be an effective way of stopping unwanted contact. However, it is important to be aware that some children may not want to do this and will see this as a last resort for both practical and social reasons.

Consider bystanders. In cyber-bullying, bystanders can easily become perpetrators – by passing on or showing to other images designed to humiliate, for example, or by 'liking' or commenting on a post. They may not recognise themselves as participating in bullying, but their involvement compounds the misery for the target. It is recommended

Contain the incident. Some forms of cyberbullying involve the distribution of content or links to content, which can exacerbate, extend and prolong the bullying. It is challenging to contain this when the content may be spread across numerous sites and networks. The quickest and most effective route to getting inappropriate material taken down from the web will be to have the person who originally posted it remove it. If you know who the person responsible is, ensure that they understand why the material is hurtful and ask them to remove it. If this is unsuccessful contact the Head of Governance at the CYPES Department who will assist you in contacting the Internet Service Provider to remove the content.

Involve the wider community. Schools are advised to provide parents and carers with information about cyber-bullying policies, procedures and activities, and opportunities for becoming involved.

Self-harm

Data from the National Self-harm Registry has shown that the average person-based rate of self-harm among 10-24-year-olds was 318 per 100,000. Peak rates were observed among 15–19-year-old females (564 per 100,000) and 18–22-year-old males (448 per 100,000). Between 2007 and 2017, rates of self-harm increased by 23%, with increases most pronounced in females and those aged 10-14 years. There were marked increases in specific methods of self-harm, including those associated with high lethality.

A Journal of Adolescence report, 2017 suggests the role of the Internet has a significant factor in young people self-harm. The report highlighted three sections contributing to an increase in self-harm. This included the use of the Internet for research into self-harming practices, exploring online imagery and exposure to such images and the distinct appeal of different social media platforms for young people engaging in self-harm.

There is also a phenomenon where some young people set up new ids online in order to send themselves bullying messages- a type of digital self-harm. This issue should be considered in conjunction with the Self Harm Policy.

If a young person is considering harming themselves, they may go online to search for methods. If your monitoring software flags up a term relating to self-harm, this must be responded to as a matter of urgency, in line with Child Protection procedures.

Radicalisation

Definition. Paragraph 7 of the Prevent Duty (UK Government advice for schools) defines extremism as: 'vocal opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces.'

Statutory requirements in the UK. As a result of the Counterterrorism and Security Act 2015, specified authorities (including schools) in the UK have a duty to have 'due regard to the need to prevent people from being drawn into terrorism.' This duty includes technical monitoring for signs of radicalisation.

Does this affect Jersey? Extremist groups aim to target young people who are perhaps lonely, disenfranchised and want to feel part of a community. This can happen to any child of any background, in any geographical location who is using the internet, and Jersey is not immune.

Sexting

Definition. Sexting is a term which describes the sharing of intimate images with others, using online technologies. Sexting is an increasing phenomenon among children, even of primary age.

The Law. Creating or sending an intimate photo of a minor (if reported as a complaint by the police) is technically a criminal offence, so incidents need very careful management.

Response. If a device is involved, secure it and switch it off. Seek advice and report to your designated safeguarding officer who should follow normal child protection procedures. Factors which would be taken into account in responding to sexting incidents include: the age of the person sending the photograph and the age of the person it was sent to; whether the individual was co-coerced into sending the image; to what extent the image has been shared online and whether the child is vulnerable and if there are existing concerns.

18 rated games and films

There is a growing phenomenon of children playing adult rated first-person games such as Call of Duty or Grand Theft Auto. These games contain extreme violence, sexually explicit content, images of drug taking and other adult themes. In addition, children have access to adults from all over the world via the headset and multi-player options, which creates an added risk.

Research shows that parents often buy these games for their children, so working in partnership with parents and carers is crucial in tackling this issue.

Appendix 2- Parental Consents Form

Data Protection Permissions

St John's School is registered as a 'controller' under the Data Protection Law (Jersey) 2018. The Data Protection Law is a privacy law which means that St John's School will not release your child's or your data to a third party unless a provision of the Law is met. This form should be read in conjunction with St John's school's Privacy Notice which can be found on our school website: www.stjohn.sch.je

There are a number of occasions when we may share your child's data with third parties to help facilitate with learning, we ask you to please tick the boxes below and sign this form as a record of your consent to the following disclosures.

	Yes	No
Website/Marketing. I give permission for my child and his/her image to be used in displays and in brochures published by St John's School and CYPES (Department of Children, Young People, Education Services and to appear on the school website.		
Offsite visit/trip. I give permission for my child to take part in any planned educational visits and understand that St John's School will notify me before events take place, these trips will be offsite, but on island.		
Photography. I give permission for my child's information (name, class, year and school ID number) to be passed to Peter Trenchard Photography so that my child's image can be used on the school's management information system, SIMS and that I may also have the opportunity to purchase his/her photograph each year.		
Competition Entry. I agree for my child & his/her work and full name to be entered in competitions e.g.eisteddfod.		
Media. I give permission for my child's image/recording and name to be used by the media when the school has asked them to record individual, class or whole school activities which are of interest eg, productions, sponsored walks, visits etc.		
Social Media. I give permission for my child to appear on the St John's School & PTA Facebook & Twitter accounts when the school wishes to celebrate class or whole school activities.		
School Communication. I understand that St John's school use Sims Intouch as the way to communicate to parents and that all parents with Parental Responsibility (PR) will have access to this.		
PG Film. On occasions during school we may show films or parts of films with PG rating, these will have been previously examined by staff for suitability prior to viewing.		
PTA. (St John's School Parent Teacher Association) is a charitable body affiliated to St John's School. From time to time the PTA may contact parents through email/letter to inform them of events etc. I agree for the PTA to have access to my contact details for this purpose. The PTA does not have access to any other personal information that school holds and will not use your contact details for any other purpose.		
Starting School. I agree to the JEP publishing my child's Starting School class photo with their first name only being given to the JEP.		
Opportunities. This covers opportunities for your child to engage in which will be helpful for your child in and out of school e.g. Jersey Music Service, Jersey Sport, extra-curricular clubs etc.		

Please turn over

Government of JERSEY

	Yes	No
Withdraw Policy. I understand that I may change my consent for permissions at any time and will do so via email to St John's School.		

Emergency School Closure. If the school needs to close in an emergency e.g. snow closure, please indicate which option you would like for your child:

Walk to a friend or relative: ☐
Remain at school until collected: ☐
Walk home alone: ☐

Please be aware that if your child is taking part in any public school events, then photographs or videos may be taken by members of the audience. If you do not wish for your child to be photographed in this way, then please ensure that you formally request that they do not take part in the production. Anyone taking photographs or videos will be reminded that these are only for personal use and if they contain images of any other child then they must not be shared publicly on social media such as Facebook or Twitter or in any other way.

Child's Name: .....

Date of Birth: .....

Year/Class: .....

Parent/Carer's Signature: .....

Parent/Carer's Full name: .....

Date: .....

Updated September 2020

Appendix 3- Acceptable User Policies- Staff and Children

St. John's School's Digital Acceptable User Policy (AUP)

- I will log on using **only my** username and password and will always log off properly
- I will keep my passwords private. I understand that I can share my password with my teachers and parents, but not with my friends.
- I will ask a teacher or suitable adult if I want to use the computers.
- I will only use age-appropriate websites / apps that a teacher or suitable adult has told or allowed me to use.
- I will take care when typing words into a search engine, making sure that the words are appropriate. I will not purposely search for any content which I know is inappropriate.
- I will only download from the internet with my teacher or parent's permission.
- I will be kind, polite and responsible when I communicate with others. I will not use inappropriate language and I appreciate that others may have different opinions.
- I WILL NOT use my school email address (including Google Classroom) to sign up to any websites.
- I will think carefully when sharing information about myself. I will not share personal information.
- I will not take or share images of anyone without their permission.
- I should ensure that I have permission to use the original work of others in my own work.
- I will treat all devices, computers and IT equipment with respect and care.
- I will tell my parents or teachers (maybe with the help of a friend) if I'm unsure or worried about something on a device or the internet).
- I will tell a teacher or suitable adult if I see something that upsets me on the screen. I know that I will not get into trouble for this.
- If I receive a message from someone I don't know, I will tell an adult straight away and I **will not** reply.
- I know that if I make incorrect choices, I might not be allowed to use a computer.

Please sign for this year to agree to our school's digital AUP:

Year 1 _____ child _____ parent

Year 2 _____ child _____ parent

Year 3 _____ child _____ parent

Year 4 _____ child _____ parent

Year 5 _____ child _____ parent

Year 6 _____ child _____ parent

St John's School Primary School
Staff Acceptable Use Policy

St John's Primary School is pleased to offer the opportunity for staff across the school to be using a range of technology. The Digital Acceptable Use Policy (signed by children and parents) and Staff Acceptable Use Policy (signed by any staff member or volunteer) outline the expectations when children and adults within the school are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).
Please read the following User Agreement and sign at the end of the document.

I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Online Safety Lead (if by a child) or Headteacher (if by an adult).
I understand the responsibilities listed for my role in the school's Online Safety policy (staff please note that the 'all staff' section applies as well as any other category) and agree to abide by these.
I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, contractors, pupils or other parents/carers.
I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy.
I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head Teacher.
I will not reveal my password(s) to anyone.
I will not allow unauthorized individuals to access email / Internet / intranet / network, or other school systems.
I will not engage in any online activity that may compromise my professional responsibilities.
I will only use the approved, secure email system for any school business.
I will only use the approved school email or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
I will not browse, download or send material that could be considered offensive to colleagues.
I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / Online Safety Officer.
I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
I will not connect a computer, laptop or other device, to the network / Internet that does not have up-to-date anti-virus software.
I will not use personal digital cameras or any device with camera capabilities for taking and transferring images of pupils or staff and will not store images at home.
Staff iPads will only be used as an educational tool. Any inappropriate use of the iPad will be reported to the Deputy Head Teacher or the Head Teacher. This will be reviewed with the member of staff involved.
Images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use.
I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with or associated with my professional role or the school.
I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.

During the school day, staff should only check (or send) email when they are not teaching. Outside of the school day staff are free to check and read their email at any time, to suit their preferred working pattern.
Emails sent to staff between the hours of 6:00pm and 7:00am should be limited. Staff are not expected to check or respond to emails between these times. This curfew is applied to encourage a better work-life balance and to make staff think more carefully about the emails they are sending.
In terms of replies to both staff and parents, we expect that any emails are responded to within a 48 hour time period. It is highly inappropriate to chase someone up for a response to an email before 48 hours have elapsed. If a response is required urgently, it may be best to consider another form of contact rather than an email. Staff may not always monitor their email accounts during the school holidays, so they may not be able to respond within 48 hours.
This is a professional environment, and as such, we expect all emails to be written in a professional manner and using correct language.
With email often being our first point of contact with outside agencies, it is vital we present ourselves as well as we can. As staff at a school, we are expected to have a good knowledge of the English language and spelling. Therefore we expect some effort to be made to email using correct grammar, punctuation and spelling, especially when interacting with parents or outside individuals.
I understand that failure to comply with this agreement could lead to disciplinary action.
I will keep staff devices such as laptops and iPads password protected.
If I am working from home, I will not divulge the password to any family members or let any member of the household use the login, laptop or device for any purpose whatsoever; use a designated room or space to work from (as appropriate) and keep the device locked up and secure at all times
I will ensure personal information/ special category information (previously referred to as sensitive data) is encrypted or password protected, especially if transferring information. I will ensure the device information is transferred on is also be password protected.

Safeguarding and Maintaining as an Academic Tool
Devices belonging to the school are not to be tampered with in any manner. If an device is found unattended, it should be given to the nearest member of staff as soon as possible. Devices are an educational tool and must be treated as such.

Care and Use of iPad/ Laptop
The iPad/ Laptop screen is made of glass and is therefore subject to cracking and breaking if misused; never drop or place heavy objects (book, laptops etc.) on top of the iPad.
Do not leave the iPad/Laptop unattended and the whereabouts of the iPad/Laptop should be known at all times.
Images of other people may only be made with the written permission of the person, or parents of the person, in the photograph. This is stored on the school's admin drive.
Upon returning the iPad/ Laptop to the school, it is the user's responsibility to delete all personal materials, including pictures, passwords and e-mails from the device.
If the iPad/ Laptop is lost, stolen or damaged, the Computing Coordinator, ICT Technician, Deputy Head Teacher or Head Teacher must be informed immediately and payment agreed.

Prohibited Uses Include:
Accessing Inappropriate Materials - Staff are not allowed to send, access, upload, download, or distribute inappropriate materials.
Malicious Use/Vandalism - Any attempt to destroy hardware, software or data.

User Signature
I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies and I agree to abide by all the points above.

I wish to have an email account; be connected to the Internet; be able to use the school's ICT resources and systems.

Signature …… Date: ……

Full Name …… (printed) Job title ……