St. John's C.E. Primary School

St. John's Vision Statement

At St. John's we want everyone to grow and flourish. Our small school is a nurturing community where we can develop our gifts and broaden our horizons. We seek to do all this within the knowledge and love of God, where the values of His Kingdom guide and inspire us.

I pray that out of his glorious riches he may strengthen you with power through his Spirit in your inner being, so that Christ may dwell in your hearts through faith. And I pray that you, being rooted and established in love, may have power, together with all the Lord's holy people, to grasp how wide and long ad high and deep is the love of Christ.' Ephesians 3.16-18

'Thriving and learning as we build God's Kingdom'

Policy: E-Safety Policy

Reviewed: October 2019 Future Review: October 2020

Introduction

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures. We are currently living in an ever-changing, advancing technological world and therefore, IT and computing is an essential role in the everyday lives of children, young people and adults. Subsequently, at St John's C.E. Primary School, it is fundamental that we are teaching our children so they are equipped with key knowledge, skills and understanding in order to access technology independently and safely both in and outside of school in the wider world whilst also promoting life-long learning as technology further develops.

Key People

Designated Safeguarding Lead (DSL) team	Mrs Susan Notley – DSL Mr Joe Law, Mr. Kamran Ezel and Mrs Pat Creed - Deputy DSLs
Online-safety lead (if different)	Mr. James Stringer
Online-safety / safeguarding link governor	Mrs Sophie Gopaul
PSHE/RSHE lead	Mr Kamran Ezel
Network manager / other technical support	Mr Christos Konstantinidis
Date this policy was reviewed and by whom	October 2019 by Mr. James Stringer
Date of next review and by whom	October 2020 by Mr. James Stringer

Roles and Responsibilities

St John's C.E. Primary School is a close school community where all members of staff have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour to protect staff, pupils, families and the reputation of the school. However, as important as it is that we are all vigilant, online safety is an important aspect of strategic leadership within the school so it is both the headteacher and the governors who have

ultimate responsibility to ensure the policy and practices and practices are embedded and monitored.

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 St John's C.E. Primary School has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access will be designed appropriately 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 through explicit Online Safety sessions, PSHE and, where appropriate, during computing lessons.
- Pupils will be educated in the effective use of the Internet in research whilst also developing children's understanding that not all content on the Internet may be original and instead may be edited for a desired effect.
- As part of the Computing curriculum, all year groups have digital literacy units that have links to online safety. These units include researching and gathering information from the Internet as well as more advanced skills such as understanding our digital footprints.
- St John's C.E. Primary School will ensure that the use of Internet derived materials by staff and pupils complies with copyright law

Through ICT 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 our pupils to ensure inclusion for all and that all pupils are prepared for full participation in society.

Pupils are taught in all lessons to be critically aware of the materials/content they access online and are guided to validate the accuracy of information. Pupils are taught to evaluate what they see, as well as consider the impact the content they are accessing has, or could have, on their mental wellbeing. As children develop their knowledge and understanding of the online world, links to how information and images can be manipulated (including those that they have originally posted online themselves and how this can be used against them) are made to ensure children have the skills to fully evaluate the content they see.

We teach the Computing National Curriculum Objectives using a different range of devices to ensure that children are efficient in using different technological devices as they become ever-present in today's society. We aim to teach our computing curriculum both using iPads and laptops to develop versatility and understanding of both devices. However, we also deliver research tasks with laptops/iPads in a cross-curricular nature, including Humanities, Science and RE.

Authorised Internet Access

By explicitly authorising use of the school's Internet access, pupils, staff, governors and parents are provided with information relating to Online Safety and agree to its use (see our AUP's)

• All staff must read and sign the 'Acceptable Use Policy' before using any school ICT resource. Teachers now must also use the designated 'staff iPad'.
• Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return an Acceptable Use Policy to consent to its use
• Children will also be asked to read and sign an Acceptable Use Policy which is differentiated between Key Stage One and Key Stage Two
• Only authorised equipment, software and Internet access can be used within the school

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children both when accessing the Internet in school as well as out of school. Subsequently however, there are inappropriate and undesirable elements that must be managed if anything occurs that should not:

• If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the school office and the Online Safety Lead or other senior member of staff, who will then contact Qubic.

• Pupils (especially older pupils) should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy

All children should be aware of the adults who they can turn to for support if they come across anything unsuitable or makes them anything uncomfortable. Furthermore, children will develop their knowledge and understanding of the fact that if this situation arises, the appropriate adult is there to help them and should not attempt to deal with a sensitive issue themselves.

Email

- Pupils do not use the LondonMail / PupilMail system from LGfL for all school emails
- Staff at this school use the Microsoft Outlook system for all school emails

Both these systems are linked to the USO authentication system and are fully auditable, trackable and managed by LGfL on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email is the only means of electronic communication to be used between staff and parents (in both directions). Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email.
  - If data needs to be shared with external agencies, USO-FX and Egress systems are available from LGfL.
  - Internally, staff should use the school network, including when working from home when remote access is available via the remote server for the school.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Pupils and staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

Digital Images

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For displays around the school
- For the newsletter
- For online prospectus or websites

Steps in school are followed to ensure digital images are used correctly.

- Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.
- Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).
- At St John's, no member of staff will ever use their personal phone to capture photos or videos of pupils and instead, school cameras and password-protected iPads will be used instead which will not leave school premises.
- Photos are stored on the school shared network in line with the retention schedule of the school Data Protection Policy.

- Staff and parents are reminded frequently about the importance of not sharing without permission, due to reasons of child protection, data protection, religious or cultural reasons, or simply for reasons of personal privacy.
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children
- Older pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social network

Social networking Internet sites provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact:

- The school will block/filter access to social networking sites and newsgroups unless a specific use is approved
- Pupils will be advised never to give out personal details of any kind which may identify themselves, other pupils, their school or their location
- Pupils will be advised not to place personal photos on any social network space in their termly safety lessons
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications
- Pupils should be encouraged to invite known friends only and deny access to others
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The Governors will consider taking legal action, where appropriate, to protect pupils, staff and the reputation of the school itself against cyber bullying and defamatory comments
- Parents will be regularly reminded not to publish images from school on social media platforms
- Pupils/students are not allowed to be 'friends' with or make a friend request to any staff, governors, volunteers and contractors or otherwise communicate via social media.
- Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online.
- Staff should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

Sexting

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. Staff other than the DSL must not attempt to view, share or delete the sexting image or ask anyone else to do so, but to go straight to the DSL who will deal with the situation in line with the safeguarding policy. The DSL will also decide on the appropriate course of action and assess the risk posed to the child or children involved and whether this required the involvement or requires a referral being made to the police and/or children's social care.

Mobile Phones/Personal Devices

Many mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils/students are not allowed to bring mobile phones into school. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- All staff who work directly with children should leave their mobile phones on silent in the staffroom and only use them in private staff areas during school hours.
- Staff may use mobile phones in emergency situations when out of school on a trip
- Child/staff data should never be downloaded onto a private phone.
- If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- Volunteers, contractors, governors should leave their phones in their pocks and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos.
- Parents are asked to leave their phones in their pockets and turned off when they are on site. Parents are asked to send urgent messages to the office which will then be passed onto the relevant and appropriate member(s) of staff.
- Parents must not use mobile phones on premises, including at school events such as celebration assembly.

School website content

The school website is a valuable source of information for parents and potential parents but again to ensure online safety, the following protocols are followed:

- The headteacher has overall editorial responsibility and ensure that content is accurate and appropriate
- No personal information for anybody will ever be shared
- Pupils' full names will not be used in association with photographs
- Pupil pictures are only published once parents have given their permission for us to do so

Personal Data

Personal data will be recorded, processed, transferred and made available according to GDPR regulations and the Local Authority Data Protection Officer's advice/recommendations.

CEOP (Child Exploitation and Online Protection)

All pupils, staff and parents should be made aware of the CEOP report button. CEOP is a law enforcement agency and is designed to keep children safe. All staff should be aware of what constitutes a CEOP report and all pupils should be aware of CEOP, the service they provide, what constitutes a report (and what does not) and what happens once a report is made.