St John's C.E. Primary School

Online Safety Policy

Our vision:

"Shaping Lives, Shaping Futures"

"Start children off on the way they should go, and even when they are old, they will not turn from it" Proverbs 22:6

The Importance of Online Safety

In the current climate of our society, many things revolve around the use of the internet. The internet is a wonderful tool, when used appropriately, however the internet can also be a dangerous place. Teaching the children, not only how to use the internet appropriately, but how to stay safe whilst using the internet is imperative. By doing so, our children will not only have the tools to stay safe online but will also have the skills to access long-life learning and employment.

Computing 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 computing within our society as a whole.

Whilst exciting and beneficial all users need to be aware of the range of risks associated with the use of technologies.

At The Spire Church of England Learning Trust (The Trust) we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet related technologies.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of fixed and mobile internet technologies provided by the Trust and/or school. Any visitors using their own devices within school adhere to the Trust's Acceptable Use Agreement and this e-safety policy.

Our Statement of Intent for Online Safety

Our pupils are regularly taught about how to keep safe whilst online to enable them to use the internet appropriately.

In particular they are advised to:

- Keep their passwords and login details secret and the benefits of changing their password regularly
- Not share any personal information
- Tell an adult if anything upsets them or makes them feel uncomfortable whilst they are online
- Only chat and communicate with people they know in real life

- Print out or screenshot any malicious or insulting messages they receive to show an adult they trust
- Be aware that anything they say or post online can be tracked back to them
- Follow the principles of the school's own online safety policy, which they have signed personally

Roles and Responsibilities

As online safety is an important aspect of strategic leadership within the school, the Trust, Head and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named online safety co-ordinators at St. John's CE Primary School are:

- Computing and e-safety co-ordinator: Charlotte Radford
- ICT manager: Sean Chadwick
- IBS Schools for internet filtering

This policy, supported by the Trust's acceptable use agreement, is to protect the interests and safety of the whole school community.

Requirements as set out in Keeping Children Safe in Education. Full detail can be found in the school safeguarding policy.

- DSLs will access appropriate training and/or support to ensure they understand the unique risks associated with online safety, can recognise the additional risks learners with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep children safe online.
- All staff will be provided with online safety information and training at induction
- All staff will receive online safety training as part of regular (at least annual) child protection training
- Staff will receive updates on online as required
- Children will be taught about online safety, including as part of statutory Relationships and Sex Education (RSE)
- The individual schools within the Trust recognise that a one size fits all approach may not be appropriate and a more personalised or contextualised approach for more vulnerable children e.g. victims of abuse and SEND, may be needed.
- We recognise that child on child abuse and child and child sexual violence and sexual harassment can occur online. Full detail can be found in the school's Anti-bullying policy.
- DSLs from all schools within the Trust will ensure they have accessed the UKCIS 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' guidance and are familiar with its content and when it should be followed.

Managing the School Online Safety Measures

We endeavour to embed online safety messages across the curriculum whenever the internet and/or related technologies are used. These messages will be appropriate to the age of the children being taught.

Online Safety guidelines and the SMART rules will be prominently displayed around the school.

As a school, each year, we also take part in various online safety activities including the participation of the national Safer Internet Day.

Security, Data and Confidentiality

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the Trust's/school's Online Safety Policy.

When assessing, amending and saving any data or information, relating to the school or pupils, school staff follow the guidelines set out in the General Data Protection Regulations 2018.

Managing the Internet

All internet activity within school is monitored and filtered through IBS Schools Smoothwall cloud based system and Impero. Whenever any inappropriate use is detected, the ICT Manager is notified and the incident will be followed up in line with the school Acceptable Use Policy.

The school maintains students will have supervised access to internet resources (where reasonable) through the school's digital devices.

If internet research is set for homework, staff will remind students of their online safety training. Parents are encouraged to support and supervise any further research.

Infrastructure

Our internet access is provided by Adept and monitored by Netbuilder. The ICT Manager manages the administrative devices throughout the school and the curriculum access.

Staff and students are aware that should they encounter or access anything unsuitable or damaging they must report it immediately to teachers, online safety co-ordinator or the ICT Manager.

Mobile Technologies

Personal Mobile Devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use during designated times outside of the classroom. They are **not** to be used at any time whilst children are present.

Personal mobile devices have access to the internet via the school's WiFi network.

The school is not responsible for the loss, damage or theft of any personal mobile device.

Managing Email

The use of email within school is an essential means of communication for staff. Pupils currently do not have access to individual email accounts within school.

Staff must use the school's approved email system for any school business, this includes any communication with parents/carers.

Staff must inform (the online safety co-ordinator/line manager/ICT Manager) if they receive an offensive or inappropriate email.

Social Networking

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day.

The school also strongly discourages children from using age inappropriate social networking outside of the school. Should the staff be made aware of incidents or activities on these social networks, which has a direct effect on the children's behaviour or attitudes within school, then the school reserves the right to take action regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

Facebook/Social Media Groups

It is not acceptable to publicly criticise or blame school management and colleagues at any time; especially through any social media including internet "blogs", websites or social networking tools such as Facebook or Twitter and you must be aware that the laws governing defamation, breach of copyright, etc. apply equally to "blogging" as to other forms of communications. Offensive, defamatory, discriminatory or otherwise inappropriate comments will not be tolerated and may constitute a disciplinary and/or criminal offence, as could the disclosure/publication of any confidential or personal information about the school, its staff, pupils or other members of the school community.

Safe Use of Images

Creation of Videos and Photographs

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

All staff are aware of specific children (they have the responsibility for) in school which do or do not have photograph permissions. If they do have permission, staff are aware of which platforms they can be used on.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes field trips. School's own mobile devices must be used in this case.

Publishing Pupil's Images and Work

All parents/guardians will be asked to give permission to use their child's work/photos in publicity materials or on the school website, school social media accounts or mobile app.

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

Pupils' names will not be publishes alongside their image and vice versa on the school website, school social media accounts, mobile app or any other school based publicity materials.

Storage of Images

Images/films of children are stored securely on the school server and/or teacher's individual encrypted devices for the length of the time the pupil remains at St. John's, normally 7 years (from Year Reception to Year 6).

Misuse and Infringements

Complaints

Complaints or concerns relating to e-safety should be made to the online safety co-ordinator, line manager or the ICT Manager.

Inappropriate Material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the online safety co-ordinator or the ICT Manager.

Deliberate access to inappropriate materials by any user will lead to the incident being logged, in the first instance, by the ICT Manager and then forwarded to the online safety co-ordinator. Depending on the seriousness of the offence, investigation may be carried out by a member of SLT. Staff are aware that negligent use or deliberate misconduct could lead to disciplinary action.

Online Safety in the Curriculum

The school provides opportunities within PSHE and computing lessons to teach about online safety, as well as explicit online safety lessons.

Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the computing curriculum.

The teaching of online safety focuses on helping children to recognise inappropriate content, conduct, contact and commercialism and helps them learn how to respond or react appropriately.

Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues.

Pupils know how to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Childline/CEOP report abuse button.

Expectations for Attainment

The expectations for our children are to become safe users of internet accessible devices. They will know how to use the internet in a safe manner, keeping themselves protected and understanding how to support themselves and peers around them to stay safe online.

Implementation of the teaching of Online Safety

EYFS

In Reception the focus for online safety is to ensure that the children are not over using devices which are online. The main message for the children in Reception is to stay safe when using any technical device, whether this be their own devices or their family members. The lessons are done through the use of stories where the children can relate to the stories' problems and issues.

Key Stage 1

In Key Stage 1, the children are immersed to more online safety issues where the children may encounter them on their own devices, such as online games. The children will be recapping the 'SMART' rules and focusing on each element of the SMART rules. It is important to get children into the habit of keeping their identity safe online by using user names and avatars.

Due to the age of the children, we teach the children to simply turn over their tablet or close their laptop screen and to tell a trusted adult if they come across anything which is upsetting. It is important to let the children know that they might come across things on the internet which may upset them but teach them the skills to deal with it.

Key Stage 2

In Key Stage 2, the children look at online safety in a more personal manner, looking at issues and problems which we know the children come across. In Key Stage 2, we know that more of our children have their own devices which are connected to the internet, often in their own bedrooms away from parental view.

In Lower Key Stage 2, the children focus on online safety through different games, using their gaming consoles as well as tablets, laptops and phones. A key message that we share with our children is that they will never be in trouble for sharing their experiences, particularly with games that are above their age. Age rating is something which we share with the children and the importance of it but also the importance of talking to a trusted adult about anything which is worrying them. When teaching online safety, teachers have an open classroom so the children feel they can talk about anything and share any issues.

In Upper Key Stage 2, the children focus more on online safety through apps and social media. Even though a lot of the apps and social media platforms that our children access have an age rating of 13+, they are still accessing them. For this reason, we teach the children how to be safe online if they are going to use these platforms. The children learn more about the technical vocabulary and the darker use of the internet, such as scams and identity theft. It is important that our children receive these lessons as they are actively using the platforms, so are regularly opening themselves up to these issues.

Embedding Online Safety across the Curriculum

There are opportunities for embedding online safety through other subjects in the curriculum whenever an internet device is being used. Whenever the lesson involves the iPads or netbooks, particularly for research purposes, the online safety rules are recapped with the children understanding how to stay safe online during that lesson.

Lesson Planning

The teaching of online safety happens once a half-term throughout the school year. The lessons are planned to suit the year group age and what online safety issues they may come across. The lessons are planned to ensure the basics are covered, like our school online safety rules, as well as teaching them technical terminology which may help to protect them in the future.

The specific online safety lessons are taught explicitly, however online safety is also taught informally through PSHE and other computing lessons when and if a question arises.

The school follows the online safety national calendar, ensuring that national online safety days and nationwide events are taught and taken part in.

Home Learning

The teaching of online safety is taught to be able to use in school, but also to be applied outside of school. A lot of the online safety teaching refers to use of technology outside of school, using their own personal devices. Due to the nature of online safety, it is important that as a school we share any knowledge with the wider school community. Involving the parents in their children's online safety lessons is done through online safety open afternoons, updates through social media as well as important messages going home through the use of the newsletter and parent mail.

We openly encourage the children to speak to a trusted adult if there is anything online which concerns them, which often lends itself to children and parents coming into school for further support. This is something which we will help with as much as we can. From this, our curriculum and lessons may change to make sure we are staying up to date with current concerns/problems.

Assessment

Assessment in online safety is to ensure our children can confidently and safely use technology. The children should be able to leave St. John's Primary School equipped with the skills to use personal devices and applications securely when they reach the age to do so. Assessment is completed through the use of pupil voice alongside the teacher's own assessment which is conducted through the use of speaking and listening.

POLICY ADOPTION

Date policy adopted …………………………………….

Signed ………………………………………………… Print Name ………………………………………………

Review date ……………………………………………..

Appendix 1

Mobile Phone and Smart Technology at St John's

Schools within the Trust recognise that mobile phones are a part of everyday life and, for parents who choose to allow their children to bring mobile phones to school, the following policy will apply. All pupils bringing mobile phones to school require parental permission.

Responsible Use

Pupils are only allowed to use mobile phones at the end of the school day once they have left the premises. Pupils will not be allowed to use phones on school premises before school or at any time during the school day.

Pupils will be responsible for their own phones and whilst the Governors give permission for phones to be brought to school, they will not take any financial responsibility for phones that are lost, damaged, stolen or confiscated.

Pupils must ensure that files stored on their phones do not contain any inappropriate material. Pupils who fail to follow this will have their phone confiscated and both their parents and the police will be informed.

Cyber-bullying is completely unacceptable. Pupils involved in this will have their phone confiscated; it will be returned to their parent/carer, or passed to the police depending on what has been reported. The consequence for this offence could result in serious consequences. Additional detail can be found in the anti-bullying policy, safeguarding policy and Behaviour and relationships policy.

Phones must be switched off (not just on silent) and out of sight at all times whilst on the school premises.

Checks and investigation will be carried out where reports are received of Pupils using their phones while in school.

Where pupils do not follow this expectation, which is in place for safeguarding reasons and to ensure that learning is not disrupted, the phone or smart device will be confiscated. On the first occasion the phone or smart device may be collected by the student at the end of the day. On any subsequent occasions the phone will be held at reception until collected by the parent/carer.

Pupils who do not follow this expectation for a third time will not be permitted to bring the phone or smart device for a given amount of time.

Parents should continue to phone reception in order to contact their children in a genuine emergency and any messages will be given to the student. Please do not try to communicate with your child during the school day via their mobile phone.

Pupils need to acknowledge that it is a privilege to be permitted to bring mobile phones to school and nonadherence to this policy will lead to a removal of this privilege.

This policy has been devised in order to protect all children and staff within the Trust's schools from any form of abuse through the misuse of mobile phones and we would appreciate your full support with this.

Appendix 2

Online Safety - Information and support for parents and children

There is a wealth of information available to support children, parents and carers to keep safe online. The following list is not exhaustive but should provide a useful starting point: Support for children

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse Parental support
- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world