St John's C.E. Primary School

E Safety Policy

May 2019

St John's C.E Primary School

The Spire Church of England Academy Trust

January 2019

Vision Statement

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

Our vision is rooted in our core values of:

Love Friendship Truthfulness Forgiveness

We promote:

- An inclusive and nurturing ethos where children can grow in confidence and knowledge in order to achieve their full potential both academically, socially and morally.
- An engaging and inspiring curriculum that meets the needs of our pupils and fosters a lifelong love of learning.
- Positive relationships and a developed moral understanding for all of our pupils.
- Independence and resilience to allow pupils to achieve their potential
- Self-belief, motivation and a desire to aim high.
- A collaborative approach between parents, school and the local community with the children at the centre.

The Spire Church of England Learning Trust

School: St. John's CE Primary School

E-Safety Policy

Computing and the use of digital devices is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Computing and 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 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 these 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 and 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.

Roles and Responsibilities

As e-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 e-safety co-ordinators at:

St John's CE Primary School are:

- Computing coordinator; Charlotte Shepherd
- E Safety Co-ordinator, Sam Strand
- 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.

Managing the school e-safety messages

We endeavour to embed e-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.

E-safety guidelines and the SMART rules will be prominently displayed around the school.

As a school, each year, we also participate in e-safety activities during Safer Internet Day.

E-safety in the Curriculum

The school provides opportunities within PSCHE and Computing lessons to teach about e-safety.

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

The teaching of e-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.

Security, Data and Confidentiality

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

When accessing, 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 e-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 school and curriculum access also managed by the ICT Manager.

Staff and students are aware that should they encounter or access anything unsuitable or damaging they must report it immediately to teachers, e-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. These are **not** to be used at any time whilst children are present.

Personal mobile devices have access to the internet via the schools 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 have access to individual email accounts within school; however, there are policies in place to restrict sending and receiving emails. Pupil email accounts are used to access E-Praise.

Staff must use the school's approved email system for any school business.

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

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 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.

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 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, twitter account 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 published alongside their image and vice versa on the school website, twitter account, 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 time the pupil remains at St. John's, normally, 7 years (from Year Ro Year 6)

Misuse and Infringements

Complaints

Complaints or concerns relating to e-safety should be made to the e-safety coordinator, line manager or 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 e-safety coordinators or 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 e-safety co-ordinator. Depending on the seriousness of the offence; investigation maybe carried out by a member of SLT. Staff are aware that negligent use or deliberate misconduct could lead to disciplinary action.

Policy adopted by Governing Body on 20th May 2019

Reviewed	April 2019
Next Review	April 2020