St John's RC

E-Safety Policy
Revised January 2016

This policy should be read alongside the schools Acceptable Use Policy

Our Mission Statement

Love of learning

and playing together

one community

aiming high

helping each other

and praying together

On our journey with Christ

Introduction

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside school.
The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone.
These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

School internet access will be designed expressively for pupil use and will include filtering appropriate to the age of the pupils. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge, location, retrieval and evaluation.

Safe and appropriate use of the internet will be the responsibility of all stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and pupils themselves.
The use of these exciting and innovative tools in schools and at home has been shown to raise educational standards and promote pupil achievement. However, the use of new technologies can put young people at risk within and outside the school. Many of these risks reflect situations in the offline world and it is essential that this e-safety Policy is used in conjunction with other school policies, e.g. behaviour, anti-bullying and child protection policies.

As with all risks, it is impossible to eliminate them completely. It is therefore essential, through good educational Provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

St John's RC Primary School has endeavoured to provide the necessary safeguards to help to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe whilst using the internet and other communication technologies for educational, personal and recreational use.

Scope of the Policy

This policy applies to all members of the school community (including staff, students/ pupils, volunteers, parents/carers, visitors) who have access to and are user of school ICT systems, both in and out of school.

The Education and Inspections Act (2006) empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

Managing Internet Access

1. Information System Security

Schools ICT systems capacity and security will be reviewed regularly. Access to network drives will be user password protected, and all staff will save data responsibly. Virus protection will be updated frequently.

Email and Messaging

Pupils may only use approved email accounts of the school system. Pupils must immediately tell a member of staff if they receive an offensive email or message. Pupils must not reveal personal details of themselves or others in email communication or messages, or arrange to meet anyone. Emails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. Staff must not give pupils or parents/carers personal email contacts, all correspondences should be done through the school office with the permission of the head teacher.

Published Content and the School Website

The contact details on the website should be the school address, email and telephone number.

Staff or pupils' personal information will not be published. The school will have overall editorial responsibility and ensure content is accurate and appropriate, adhering to the Data Protection Act (1998). Written permission is obtained from parents/carers before photographs/videos are published on the school website. Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Images of Pupils

The school will avoid identifying a pupil by name (unless for a specific reason, such as an award of recognition, and in such cases only using a first name), exclude any images of

children where parents/carers have specifically requested no images should appear (e.g. in child protection cases), only show images of pupils fully clothed, and will always give parents/carers the right to have an image removed.
When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. social networking sites. Pupils must not take, use, share, publish or distribute images of others without their permission.
Staffs are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

Social Networking and Personal Publishing

The school will block/filter access to social networking sites. The use of instant messaging or chat will not be permitted in any online capacity e.g. via games online or apps. Pupils will be advised never to give out personal details of any kind which may identify their location. Pupils will be advised of appropriate and inappropriate message conduct. Pupils will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Child Protection

Misuse of information technology (e.g. sexting, inappropriate comments on Facebook, cyber bullying or online grooming) is recognised and dealt with in the school's Child Protection Policy. Children are specifically taught about e-safety and cyber bullying in the curriculum.

Managing Filtering

The school will work with the LA, DfE and the Internet Service Provider to ensure systems protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the E-safety Coordinator immediately. Senior staff will ensure that regular checks are made to ensure the filtering methods selected are appropriate, effective and reasonable.

Procedures for Whole School

Authorising Internet Access

All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up to date, for instance a member of staff may leave or a pupil's access be withdrawn. In Foundation Stage, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials. Parents/carers will be asked to sign and return a consent form.

Assessing Risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is

not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access. Any pupil who discovers such material must immediately report it to a member of Staff, who will inform the e-safety coordinator.
The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective. All teachers and teaching assistants will be trained on how to minimise and manage any potential e-safety risks.

Handling E-Safety Complaints
Complaints of internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the head teacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

E-Safety Policy Communications

Introducing the E-Safety Policy to Pupils
E-safety will be taught as part of the ICT curriculum and included as part of PSHE; this will cover both the use of ICT and new technologies in school and outside school. Key e-safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities. Pupils will be taught in all lessons to be critically aware of the materials/content they access online 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.
Rules for use of ICT systems/internet will be displayed and referred to around school. Pupils will be informed that networks and internet use will be monitored.

Staff and the E-Safety Policy
All staff will be given the school's e-safety policy, will sign the Staff Acceptable Use Policy, and have its importance explained. They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regards to these devices. They will be kept up to date of e-safety matters and of the current school e-safety policy and practices. Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
Staff should ensure that lessons where internet is used are 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.

Enlisting Parent/Carer Support
Parents/carers' attention will be drawn to the school e-safety policy in newsletters and on the school website. They will be invited to parents' meetings to discuss e-safety and attend e-safety workshops and assemblies.

Failure to Comply
Failure to comply in any way with this policy will be considered a serious risk to health and safety and all incidents of non-compliance will be investigated by a senior member of staff.

Appendices

Pupil Acceptable Use
Parent Consent
Staff Acceptable Use