St John Rigby Catholic Primary School E-Safety Policy

God's Will Be Done Through Work and Play as we Follow Jesus Day by Day.

Introduction

The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to e-safety. The policy relates to other policies including ICT curriculum and Internet Access, Bullying, Child Protection and Health and Safety.

This policy sits alongside the SFAAT overall online Safety policy which outlines wider approaches taken to ensure safe internet and ICT use across the schools. It also contains bespoke copies of the Acceptable Use agreements. Some of these, which are bespoke to St. John Rigby feature at the end of this policy.

Writing and reviewing the e-Safety policy

The school has a designated e-safety co-ordinator (Ms Zoey Diemer).
The e-Safety policy has been agreed by the Headteacher and staff and approved by the governors. It will be reviewed on an annual basis.

Date to be revised: October 2017

Teaching and Learning

The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management, information and business administration systems.
Access to the Internet is a necessary tool for staff and students.
It helps to prepare students for their on-going career and personal development needs.
It is a requirement of the National Curriculum (NC) orders for ICT and the Computing Curriculum and is an integral part of teaching and learning in all subject areas.

Internet use enhances learning. Internet access is provided by TalkStraight and is designed for pupils. This includes filtering appropriate to the content and age of pupils. Internet access is planned to enrich and extend learning activities. Access levels are reviewed to reflect the curriculum requirement. Teachers select sites which support the learning outcomes planned for pupils' age and maturity. Filtering is carried out by LightSpeed systems which is under the control of TalkStraight.

Pupils are taught how to take responsibility for their own Internet access and are given clear objectives for Internet use.

- Pupils are taught how to evaluate Internet content and how to validate information before accepting that it is necessarily accurate.
- Older pupils are taught to acknowledge the source of information, when using Internet material for their own use.
- Pupils are made aware that the writer of an e-mail or the author of a Web page might not be the person claimed.
- Pupils are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

Managing Internet Access

Information System Security

The school ICT system security is reviewed regularly and Virus protection is updated regularly. Security strategies are discussed with the school's service provider, Perspective Education.

E-mail

- Pupils are allowed to use school email accounts only.
- Pupils must tell a teacher immediately if they receive an offensive email.
- In emails, pupils are taught that they must not reveal their personal details, those of others or arrange to meet anyone without specific permission.
- Pupils are taught not to open suspicious incoming email or attachments.

Published content and the school web site and social media sites

The website complies with the school's guidelines for publications.
Occasionally we may celebrate our children's achievements by publishing their work on the school website or social media sites. Pupils are taught to consider the audience and purpose for the work they publish on the school website and ensure their work is of high quality.
All material must be the author's own work or where permission to reproduce has been obtained, it is clearly marked with the copyright owner's name.

Publishing pupils' images

- Images may be used on display walls in school or in the school prospectus

- Photographs will not identify individual pupils. Group shots or pictures taken "over the shoulder" are used in preference to individual "passport" style images.
- Children's photographs are only allowed to go on the website once written permission has been received from the child's parents. Parents will be asked to sign a form at the beginning of each school year giving permission. Photographs will be removed at parent's request
- Children's photographs are not accompanied by names.
- Children's work which contains photographs will not contain the child's name.
- LAC images are never used in any publications or the website unless express permission is granted by the child's carer.

Social networking and personal publishing

Pupils and staff will not be allowed to access public chat rooms or social networking sites in school. The service provider/school will block/filter access to social networking sites, except those specifically purposed to support educationally approved practice. The Senior leadership team have access to the School's Twitter/Facebook account which is designed to give parents updated information. Any attached content follows the same procedures as website content.

Managing filtering

The school works in partnership with parents, the Internet Service Provider and the school's managed service (Partnership Education) to ensure systems to protect pupils are reviewed and improved.
Senior staff will ensure that checks are made to ensure that the filtering methods selected are effective in practice.
If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT/E-safety co-ordinator.

Managing emerging technologies

Mobile phones should not be brought to school by pupils. We recognise that our oldest pupils may walk on their own to and from school and parents may wish them to have a mobile phone for emergencies. However we discourage this on security grounds as they are easily lost, damaged or stolen. Pupils are taught that they shouldn't have a mobile phone on their person in school and that any phone brought in must be handed to the office for the duration of the day. The sending of abusive or inappropriate text messages is forbidden.

Staff mobile phones should not be used during lesson time or when supervising pupils. Personal mobile phones should not be connected to the school network. Cameras in mobile phones are not to be used by staff or pupils. Only school cameras are used by both staff and children for educational purposes. Cameras should not be used by parents on school premises without permission from the Headteacher.

Any photographs that contain images of children other than your own must not be published on websites or social networking sites.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
Staff must not keep confidential information on removable devices such as USB devices unless suitably security protected.
Obsolete computer hardware will be destroyed.

Policy Decisions

Authorising Internet access

All staff must read and sign the "Staff code of conduct for ICT" before using any school ICT source. The school maintains a record of all staff and children who have access to the school's ICT systems.
Parents are asked to sign a consent form regarding their child's internet use (see Acceptable Use Policy).
Any person not directly employed by the school will be asked to read and sign the "acceptable use of school ICT resources" before being allowed to access the internet from the school site.

Assessing risks

The school takes all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school, SFAAT or TalkStraight can accept liability for any material accessed, or any consequences of Internet access. The school's e-safety policy and its implementation will be monitored and reviewed on a regular basis.

Handling online safety complaints

Complaints of internet misuse must be referred to the Headteacher.
Any complaint about staff misuse must be referred to the Headteacher.
Complaints of a child protection nature must be dealt with in accordance with the school's child protection policy.
Pupils and parents are informed of the complaints procedure.
Pupils and parents are informed of the consequences for pupil misuse of the Internet (see Acceptable Use Policy).

Communications Policy

Introducing the online safety policy to pupils

Online safety posters are posted next to all computers so that all users can see them.

Pupils are informed that network and Internet use is monitored and appropriately followed up.
The children receive e-safety lessons and are constantly reminded of online safety.

Staff and the online safety policy

All staff are trained regularly and receive a copy of the online safety policy.
Staff are informed that network and Internet traffic can be traced to an individual user. Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

Parents' and carers' attention is drawn to the school's online safety Policy in newsletters, the school brochure and on the school website.
The school asks all new parents to sign the pupil/parent agreement when they register their child with the school.
The school provides information sharing (bulletins, links, letters for specific year groups, workshops) for parents in order to update them on developments and offer support in ensuring that their children are safe when online outside of school.

Incident Log

FBCS
E-Safety Incident Log

Details of ALL E-Safety incidents to be recorded by the SIRO (Senior Information Risk Owner).

This incident log will be monitored termly by the Head Teacher, member of the SLT or Chair of Governors. Any incidents involving Cyber bullying should be recorded on SIMS Behaviour Log following guidance provided by Bedford Borough Council

Date & time	Name of student or staff member	Male or Female	Room and computer/device number	Details of incident (including evidence)	Actions and reasons

ICT Acceptable Use Agreement: Staff, Volunteers, Governors and Visitors

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the SIRO (Senior Information Risk Owner) or Head Teacher.

- I will only use the school's email/Internet/Intranet/Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head Teacher or Directors.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to children.
- I will only use the approved, secure email system for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware of software without permission of the SIRO.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of children and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Head Teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head Teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help children to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …….…… Date ……

Full Name …….....(printed)

Role . . . . . .

Access to SIMS Learning Gateway - staff user agreement

Access to SIMS Learning Gateway (SLG) is covered by the terms of the Data Protection Act. This includes a legal expectation that data held by school will be kept secure. This means that it must not be viewed, copied or downloaded by any member of the public.

Information security breaches may cause real harm and distress to the individuals they affect – lives may even be put at risk. Examples of the harm caused by the loss or abuse of personal data (sometimes linked to identity fraud) include:

- fake credit card transactions;
- witnesses at risk of physical harm or intimidation;
- offenders at risk from vigilantes;
- exposure of the addresses of service personnel, police and prison officers, and women at risk of domestic violence;
- fake applications for tax credits; and
- mortgage fraud.

Not all security breaches have such grave consequences, of course. Many cause less serious embarrassment or inconvenience to the individuals concerned. Individuals are entitled to be protected from this kind of harm as well.

Data which is accessed from home is clearly more likely to be seen by someone who is not authorised to view the data. Consequently it is essential that all staff understand their responsibility to ensure the security of the data including abiding by the requirements below.

1. Access to SLG for individual members of staff is entirely at the discretion of members of the Senior Management Team.

2. SLG may only be accessed from school equipment. Outside of school this means it may only be accessed from a School laptop.

3. Before SMG can be accessed the school laptop must have a valid health and safety check. This is an annual check carried out on school premises and access to SLG is dependent upon this.

4. Anti-virus software must be kept up to date on the laptop.

5. The laptop may only be used by the member of staff who has signed to say they are responsible for the laptop.

6. The laptop must be locked if the user steps away from it for any reason no matter how quickly you expect to return; ideally you should log out of SLG.

7. Do not access SLG in any place where the information could be seen by anyone who is not a member of the school staff with a legitimate reason for accessing the data themselves. For example, do not access SLG in front of a member of your family, a friend or in front of a window.

8. Do not access SLG via an Internet connection you are not absolutely sure is secure i.e. do not use an Internet hotspot, a hotel Internet connection etc. Use a router/switch which is protected by a firewall.

I agree to abide by these requirements. I understand that I am responsible for my own actions and as such a breach of security which happens as a result of my actions is my responsibility.

Signed: Date:

Name (please print):

ICT Acceptable Use Agreement: Children

1. I will only use ICT systems in school for school work.
2. I will only log on to the school network with my own user name and password.
3. I will follow the schools ICT security system, not reveal my passwords to anyone and change my passwords regularly.
4. I will only use my school email address.
5. I will make sure that all ICT communications do not upset or embarrass anyone.
6. I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
7. I will not give out any personal information such as name, phone number or address.
8. I will not take copies of photos from the school network.
9. I will respect other people's work at all times. This means that I won't copy from anyone else and I won't try to delete or change their work either. I will only touch my own computer and will not in any way interfere with a computer being used by someone else.
10. I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

Signed …….

Class……. Date …….

date

Dear Parent/ Carer

ICT Acceptable Use Agreement

ICT, which includes the Internet, learning platforms, email and mobile technologies, has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT. It is essential that children are aware of potential risks and know how to keep themselves safe.

Please read and discuss the attached ICT Acceptable Use Agreement with your child then sign and return the reply slip to school. Any concerns can be discussed with their class teacher.

All classes will begin their ICT lessons each year by considering how to stay safe when using ICT. All year groups will focus on the Acceptable Use Agreement; ensuring children understand aspects pertinent to them. Over the course of the year children will consider how they can communicate safely and effectively within the school and with other schools under the direct supervision of the teacher. KS2 students will look at the potential dangers of meeting new friends on-line with a clear emphasis on how to stay safe.

There will be a parent workshop early in the Autumn Term which will seek to raise awareness of potential risks and how to keep children safe when using ICT.

Thank you for your support with this matter.

Yours sincerely

name
Headteacher

ICT Acceptable Use Agreement

We have discussed this document and ……..... (student name) agrees to follow the ICT Acceptable Use Agreement and to support the safe and responsible use of ICT at St **name** School.
Parent/ Carer Signature

……...……

….....

Pupil Name / Signature

…….....
....

Class ……..... Date

…….....