St John's RC Primary School

E-Safety Policy
September 2016

1. Introduction

1.1 MSCB guidance – **Safeguarding Children in the use of electronic media,** has been used to inform this policy. MSCB's principles of best practice have been taken into consideration when producing this e-safety policy and also our 'Acceptable Use Policy' here at St John's School.

1.2 This policy has been developed to ensure that all adults in St John's R.C. Primary School are working together to safeguard and promote the welfare of children and young people.

1.3 E-Safety is a safeguarding issue, not a Computing issue, and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

1.4 This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities by using computer technology, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

1.5 The Head-teacher or, in their absence, the authorised member of staff for E-Safety, has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

1.6 This policy complements and supports other relevant school and Local Authority policies.

1.7 The purpose of internet use in school is to help raise educational standards, promote pupil achievement, support the professional work of staff, as well as to enhance the school's management information and business administration systems.

1.8 The internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience.

2. Ethos

2.1 It is the duty of the school to ensure that every child in its care is safe, including in the 'virtual' or digital world. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's computing facilities and digital technologies.

2.2 Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures.

2.3 All staff have a responsibility to support e-Safe practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols.

2.4 E-safety is a partnership concern and is not limited to school premises, school equipment or the school day.

2.5 Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will be dealt with in accordance with the school's Anti-Bullying and Behaviour Policy.

2.6 Complaints and/or allegations related to child protection will be dealt with in accordance with the school's Child Protection & Safeguarding Policy.

3. Roles and Responsibilities

3.1 The Headteacher will ensure that:

- All staff are included in E-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- A designated member of staff for E-Learning/Safety (The Computing Subject Leader) receives appropriate on-going training, support and supervision and works closely with the Designated Person for Safeguarding.
- All temporary staff and volunteers are made aware of the school's E-Learning/Safety Policy and arrangements.
- A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.

3.2. The Governing Body of the school will ensure that:

- There is a senior member of the school's leadership team who is designated to take the lead on E-Learning/Safety within the school.
- Procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority procedures.

3.3 The Designated Member of Staff for E-Learning/Safety (Mr E. Smithers) will:

- Act as the first point of contact with regards to breaches in e-safety and security.
- Liaise with the Designated Person for Safeguarding as appropriate.
- Ensure that all computing security is maintained.
- Attend appropriate training.
- Provide support and training for staff and volunteers on E-Safety.
- Ensure that all staff have received a copy of the school's Acceptable Use of Computing Policy document.
- Ensure that all staff understand and aware of the school's E-Safety Policy.
- Ensure that the school's computer systems are regularly reviewed with regard to security.
- Ensure that the virus protection is regularly reviewed and updated.
- Discuss security strategies with their IT technical partner when necessary.

4. Teaching and Learning

Benefits of internet use for education

4.1 The internet is a part of the statutory curriculum and a necessary tool for staff and children and benefits education by allowing access to world - wide educational resources including art galleries and museums as well as enabling access to specialists in many fields for pupils and staff.

4.2 Access to the internet supports educational and cultural exchanges between students world - wide and enables pupils to participate in cultural, vocational, social and leisure use in libraries, clubs and at home.

4.3 The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data with the Local Authority and DfE.

4.4 The internet improves access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, government initiatives.

4.5 The internet offers opportunities for mentoring pupils and providing peer support for them and their teachers.

4.6 Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of the children and young people.

4.7 Children and young people will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

4.8 Children and young people will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information. Children and young people will also be taught that copying material is worth little without an appropriate commentary demonstrating the selectivity used and evaluating the material's significance.

4.9 Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

5. Managing Internet Access

5.1 Developing good practice in internet use as a tool for teaching and learning is essential. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children and young people.

5.2 Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupil's age and maturity.

5.3 Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

5.4 If staff or pupils discover unsuitable sites, the URL (address) and content must be reported as soon as possible to the Internet Service Provider via the Computing Subject Leader.

5.5 The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

5.6 Pupils will be taught to be critically aware of the materials they read as well as how to validate information before accepting its validity.

6. Managing Email

6.1 Personal e-mail or messaging between staff and pupils should not take place.

6.2 Pupils must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.

6.3 The forwarding of chain letters is not permitted.

6.4 Incoming e-mail should be monitored and attachments should not be opened unless the author is known.

7. Managing Website Content

7.1 Editorial guidance will ensure that the school's ethos is reflected in the St John's RC Primary School blog, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

7.2 Photographs of pupils will not be used without the written consent of the pupil's parents/carers.

7.3 The point of contact on the school blog will be the school address, school e-mail and telephone number. Staff or pupil's home information will not be published.

7.4 The Headteacher, together with the Web-site administrator , will monitor the whole-school blog. Each class teacher will have responsibility for their own class blog. In addition, some members of staff also have responsibility for other individual blogs (e.g. sport, Spanish). In certain cases, non-members of staff have been given administration

rights of an individual blog (e.g. PTA, ART Club). The person with responsibility for a particular blog should ensure that all content is accurate and appropriate.

7.5 The blog will comply with the school's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing.

7.6 Use of site photographs will be carefully selected so that any pupils cannot be identified by full name or their image misused.

7.7 First names of pupils may be used on the blog, but not in association with any photographs.

7.8 Work will only be used on the blog with the permission of the pupil and their parents/carers.

7.9 The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

7.10 Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

8. Social Networking and Chat Rooms

8.1 The school will control access to moderated social networking sites (such as pupil comments on school blog) and educate pupils in their safe use.

8.2 Pupils will not access social networking sites eg 'Twitter', 'Facebook' or 'Instagram'. Pupils at St John's are not of the age of consent for these sites but we recognise some children do have accounts that they access with parental consent from home. We will seek to educate parents/children of this fact.

8.3 Pupils will be taught the importance of personal safety when using social networking sites and chat rooms.

8.4 Pupils will not be allowed to access public or unregulated chat rooms.

8.5 Pupils will only be allowed to use regulated educational chat environments and use will be supervised.

8.6 Newsgroups will be blocked unless an educational need can be demonstrated.

8.7 Staff will not exchange social networking addresses or use social networking sites to communicate with pupils.

8.8 Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a pupil is necessary, the agreement of a senior

manager should always be sought first and language should always be appropriate and professional.

9. Mobile Phones

9.1 Pupils who bring mobile phones (or any other mobile device with internet access) into school must hand them in to the class teacher at the start of the day and only collect them at the end of the school day.

9.2 The mobile phone (or similar device) must remain switched off while on school premises, this includes in both before and after care.

10. Filtering

10.1 If staff or pupils discover unsuitable sites, the URL **(address)** and content must be reported as soon as possible to the Computing Subject Leader.

10.2 Any material the school deems to be unsuitable or illegal will be immediately referred to our ISP provider.

10.3 Regular checks by our IT technical service provider will ensure that the filtering methods selected are appropriate, effective and reasonable.

10.4 Filtering methods will be selected by the school IT technical service provider in collaboration with the Computing Subject Leader and will be age and curriculum appropriate.

11. Authorising Internet Access

11.1 All staff must read and sign the school's 'Staff Acceptable Use Policy for Computing' before using any school computing resources.

11.2 The school will maintain a record of pupils whose parents/carers have specifically requested that their child be denied internet or e-mail access.

11.3 Staff will supervise access to the internet from the school site for all pupils.

12. Photographic, Video and Audio Technology

12.1 It is not appropriate to use photographic or video technology in changing rooms or toilets.

12.2 Staff may use photographic or video technology to capture / support school trips and appropriate curriculum activities.

12.3 Pupils must have permission from a member of staff before making a video or audio recording in school or on educational activities.

13. Assessing Risks

13.1 Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The senior leadership team should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

13.2 In common with other media such as magazines, books and video, some material available through the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of Internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of Internet access.

13.3 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

13.4 The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored.

13.5 Access to any websites involving gambling, games or financial scams is strictly forbidden and will be dealt with accordingly.

14. Introducing the Policy to Children

14.1 Rules for safe use of the Internet will be displayed in the Computing Suite.

14.2 Responsible Internet use, covering both school and home use, will be taught as part of the Computing curriculum. Each unit of study will include an e-safety element.

14.3 Pupils will be instructed in responsible and safe use before being allowed access to the Internet and will be reminded of the rules and risks of any lesson using the Internet.

14.4 Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.

15. Consulting Staff

15.1 It is essential that teachers and learning support staff are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies:

- All staff are governed by the terms of the school's E-safety Policy and 'Computing Acceptable Use Policy'. All staff will be provided with a hard copy and its importance explained.
- All new staff will be given a copy of the policy during their induction.
- Staff development in safe and responsible use of the internet will be provided as required.
- Staff will be aware that internet use will be monitored and traced to the original user. Discretion and professional conduct is essential.

16. Maintaining ICT Security

16.1 Personal data sent over the network will be encrypted or otherwise secured.

16.2 Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mails.

16.3 Our network management consultants, together with the Computing Subject Leader, will ensure that the system has the capacity to deal with increased traffic caused by Internet use.

17. Dealing with Complaints

17.1 Staff, children, parents/carers must know how and where to report incidents. E-safety incident forms can be located in the staff room, school office and from the safeguarding DP. Concerns related to Child Protection & Safeguarding issues must dealt with through the school's Child Protection & Safeguarding Policy and Procedures.

17.2 The school's designated person for e-safety will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the Headteacher immediately. These complaints, and/or e-safety incidents, will be investigated and logged in the 'Overview of e-safety incidents' document. The safeguarding team will regularly review this document and provide support, guidance and training based on the outcomes of these incidents.

17.3 Parents/carers and pupils will work in partnership with the school staff to resolve any issues.

17.4 As with some other safeguarding concerns, there may be occasions when the school must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.

17.5 Sanctions for misuse may include any or all of the following:

- Interview/counselling by an appropriate member of staff
- Informing parents/carers
- Removal of internet access for a specified period of time, which may ultimately prevent access to files held on the system.
- Referral to the police.

18. Parent/Carers Support

18.1 Parents/carers will be informed of this policy which may be accessed on the school website.

18.2 Any issues concerning the internet will be handled sensitively to inform parents/carers without undue alarm.

18.3 Interested parents/carers will be referred to organisations such as the Child Exploitation and Online Protection (CEOP). The CEOP website is an excellent source of information for parents/carers about how to manage e-safety outside the school setting.

This policy was ratified by the Governing Body at its meeting in **September 2016.** The policy will be reviewed again in **September 2017.**