

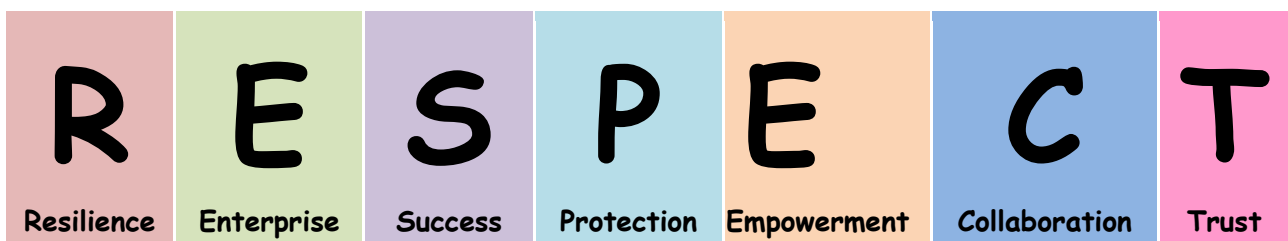


# St Ann's Junior & Infant School

## E Safety Policy

### **St Ann's Junior and Infant School Vision**

As a Rights Respecting School our vision at St Ann's is to promote **RESPECT** in everything we do... in school, Rotherham and beyond.



# Contents:

## Contents

1.  
Introduction.....**Erro**  
**r! Bookmark not defined.**  
2.Managing Internet Access .....4  
3. Policy Decisions.....7  
4.Pupil Online Safety Curriculum.....8  
5. Communications Policy.....10  
Appendix 1.....11  
Appendix 2.....12

## 1. Introduction

Protecting young people and adults properly means thinking beyond the school environment. Broadband, Wifi and 3/4G connections now mean the World Wide Web is available anywhere, anytime. Moreover, the introduction of the internet on games consoles, tablets and mobile phones mean it is becoming increasingly difficult to safeguard our children from the dangers hidden in cyberspace.

Our children will not only be working online in school or at home, their personal devices are not always covered by network protection and it is, therefore, imperative that they are educated on the risks involved with using the internet and are provided with guidance and a range of strategies on how to act if they see, hear or read something that makes them feel uncomfortable.

As a result, designing and implementing an e-safety policy demands the involvement of a wide range of interest groups: the Headteachers, Governors, Leadership Team, SENCO, Designated Safeguarding Lead, classroom teachers, support staff, young people, parents or carers, Local Authority personnel, Internet service providers (ISP), and Regional broadband consortia, working closely with ISPs on network security measures.

### **The purpose of this policy is to:**

- set out the key principles expected of all members of the school community at St Ann's J&I school with respect to the use of IT-based technologies.
- safeguard and protect the children and staff of St Ann's J&I school assist staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as online bullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

## **2. Managing Internet Access**

### **2.1 Information system security**

- St Ann's J&I school ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.

### **2.2 E-mail**

- Pupils may only use approved e-mail accounts on the St Ann's J&I school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- St Ann's J&I school should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.
- St Ann's J&I school:
  - ✓ Provides staff with an email account for their professional use (Microsoft 365) and makes clear personal email should be through a separate account.
  - ✓ Does not publish personal e-mail addresses of pupils or staff on the school website.
  - ✓ Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
  - ✓ Will ensure that email accounts are maintained and up to date
  - ✓ Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
  - ✓ Knows that spam, phishing and virus attachments can make e mails dangerous.

### **2.3 Published content and the St Ann's J&I school website**

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- The Headteachers /Deputy Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers.
- St Ann's J&I school web site complies with the statutory DfE guidelines for publications.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. info@schooladdress or admin@schooladdress. Home information or individual e-mail identities will not be published.
- Photographs published on the web do not have full names attached.

- We do not use pupils' names when saving images in the file names or in the tags when publishing to the St Ann's J&I school website.

## **2.4 Publishing pupil's images and work**

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face photos of individual children.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins St Ann's J&I school.
- Staff sign the St Ann's J&I school Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications St Ann's J&I school will obtain individual parental or pupil permission for its long term use.
- St Ann's J&I school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.

## **2.5 Social networking and personal publishing**

- St Ann's J&I school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Staff will be reminded of the risks of accepting parents and children as 'friends' on social networking sites, will be strongly advised not to do so, and given advice on how to 'block' children from viewing their private pages.
- Staff will be shown how to 'block' their profile picture from being downloaded, and protect their profile information.
- Staff will be encouraged to 'untag' themselves from any inappropriate pictures that may appear on social networking sites.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- St Ann's J&I school staff will ensure that in private use:
  - ✓ No reference should be made in social media to students / pupils, parents / carers or school staff
  - ✓ They do not engage in online discussion on personal matters relating to members of the school community
  - ✓ Personal opinions should not be attributed to the school or local authority

- ✓ Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

## **2.6 Managing filtering**

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Head Teacher.
- Blue Box will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

## **2.7 Managing videoconferencing & webcam use**

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised.

## **2.8 Managing emerging technologies**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The Senior Leadership Team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile phones will be kept under review.
- Staff will not use personal mobile phones to communicate with children, or use them to capture images of them.

## **2.9 Protecting personal data**

- Personal data will be recorded, processed, transferred and made available according to GDPR.

## **2.10 Personal devices and mobile phones**

- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded.
- St Ann's J&I school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.

- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Students' use of personal devices
  - ✓ St Ann's J&I school does not allow student mobile phones to be brought into school.
  - ✓ If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
  - ✓ If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents wishing to contact their child during the school day, should contact the school office.

### 3. Policy Decisions

#### 3.1 Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- St Ann's J&I school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At EYFS and Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

#### 3.2 Assessing risks

- St Ann's J&I school will take 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.
- St Ann's J&I school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

#### 3.3 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 Headteacher /Deputy Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with St Ann's J&I school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

### 4. Pupil Online Safety Curriculum



#### **4.1 Teaching and learning**

St Ann's J&I school has a clear, progressive Online safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to the age of the children, including:

- ✓ to STOP and THINK before they CLICK
  - ✓ to develop a range of strategies to evaluate and verify information before accepting its accuracy;
  - ✓ to know how to narrow down or refine a search (KS2);
  - ✓ to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
  - ✓ to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
  - ✓ to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
  - ✓ to have strategies for dealing with receipt of inappropriate materials;
  - ✓ to understand why and how some people will 'groom' young people for sexual reasons (KS2);
  - ✓ to understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
  - ✓ to know how to report any abuse including online bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- Teachers plan Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
  - All staff will model safe and responsible behaviour in their own use of technology during lessons.

#### **4.2 Online risks**

- St Ann's J&I school recognises that pupils increasingly use a range of technology such as mobile phones, tablets, games consoles and computers. It will support and enable children to use these technologies for entertainment and education but will also teach children (in PSHE) that some adults and young people will use such outlets to harm children.

#### **4.3 Cyber-bullying and abuse**

- Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" - DCSF 2007
- Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with St Ann's J&I school / LA child protection procedures.
- Through the PSHE curriculum, children are taught to tell a responsible adult if they receive inappropriate, abusive or harmful e-mails or text messages.

- Cyber-bullying will be treated as seriously as any other form of bullying and will be managed through our anti-bullying procedures. Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the St Ann's J&I school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.

#### **4.4 Sexual exploitation/sexting**

- Sexting between pupils will be managed through our anti-bullying procedures.
- All staff are made aware of the indicators of sexual exploitation and all concerns are reported immediately to the DSL.
- There are clear procedures in place to support anyone in the school community affected by sexting.
- All incidents of sexting reported to the school will be recorded.

#### **4.5 Radicalisation and extremism**

- Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.
- Extremism is defined by the Crown Prosecution Service as 'The demonstration of unacceptable behaviour by using any means or medium to express views which:
  - ✓ Encourage, justify or glorify terrorist violence in furtherance of particular beliefs.
  - ✓ Seek to provoke others to terrorist acts.
  - ✓ Encourage other serious criminal activity or seek to provoke others to serious criminal acts.
  - ✓ Foster hatred which might lead to inter-community violence in the UK.'
- St Ann's J&I school understands that there is no such thing as a "typical extremist": those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.
- St Ann's J&I school understands that pupils may become susceptible to radicalisation through a range of social, personal and environmental factors - it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff are able to recognise those vulnerabilities.
- Staff will maintain and apply a good understanding of the relevant guidance in order to prevent pupils from becoming involved in terrorism.
- St Ann's J&I school will monitor its RE curriculum and assembly policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.
- Senior leaders will raise awareness within the school about the safeguarding processes relating to protecting pupils from radicalisation and involvement in terrorism.

## **5. Communications Policy**

### **5.1 Introducing the e-safety policy to pupils**

- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- Safety training will be embedded within the computing and PSHE scheme of work in line with National Curriculum expectations.

### **5.2 Staff and the e-Safety policy**

- All staff will be given the school e-Safety Policy and have its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

### **5.3 Enlisting parents' and carers' support**

- Parents' and carers' attention will be drawn to the St Ann's J&I school e-Safety Policy in an e-safety leaflet, and on the school Web site.
- St Ann's J&I school will ask all new parents to sign the parent /pupil agreement when they register their child with the school

# Learning technologies in school

<b><u>Technology</u></b>	<b><u>Pupils</u></b>	<b><u>Staff</u></b>
Personal mobile phones brought into school	Pupils not allowed	Staff allowed at certain times
Mobile phones in lessons	Pupils not allowed	Staff allowed at certain times
Mobile phones outside of lessons	Pupils not allowed	Staff allowed
Taking photographs or videos on personal equipment	Pupils not allowed	With the approval of the head teacher
Taking photographs or videos on school devices	Pupils allowed under direction of staff	Staff allowed
Use of hand held devices such as PDA's, MP3's and personal gaming consoles	Pupils allowed under direction of staff to support learning	Staff allowed if use supports learning
Use of personal e-mail addresses in school	Pupils not allowed	Staff allowed at certain times
Use of school e-mail addresses for personal correspondence	Pupils not allowed	Staff not allowed
Use of on-line chat rooms	Pupils not allowed	Staff not allowed
Use of instant messaging services	Pupils not allowed	Staff not allowed
Use of blogs, wikis, podcasts.	Pupils allowed under direction of staff to support learning	Staff allowed if use supports learning
Use of social networking sites	Pupils not allowed	Staff not allowed
Use of video conferencing	Pupils allowed under direction of staff to support learning	Staff allowed if use supports learning

BBC Stay Safe

[www.bbc.co.uk/cbbc/help/safesurfing/](http://www.bbc.co.uk/cbbc/help/safesurfing/)

Becta

<http://schools.becta.org.uk/index.php?section=is>

Chat Danger

[www.chatdanger.com/](http://www.chatdanger.com/)

Child Exploitation and Online Protection Centre

[www.ceop.gov.uk/](http://www.ceop.gov.uk/)

Childnet

[www.childnet-int.org/](http://www.childnet-int.org/)

Cyber Café

[http://thinkuknow.co.uk/8\\_10/cybercafe/cafe/base.aspx](http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx)

Digizen

[www.digizen.org/](http://www.digizen.org/)

Kent e-Safety Policy and Guidance, Posters etc

[www.clusterweb.org.uk/kcn/e-safety\\_home.cfm](http://www.clusterweb.org.uk/kcn/e-safety_home.cfm)

Kidsmart

[www.kidsmart.org.uk/](http://www.kidsmart.org.uk/)

Kent Police – e-Safety

[www.kent.police.uk/Advice/Internet%20Safety/e-safety%20for%20teacher.html](http://www.kent.police.uk/Advice/Internet%20Safety/e-safety%20for%20teacher.html)

Think U Know

[www.thinkuknow.co.uk/](http://www.thinkuknow.co.uk/)

Safer Children in the Digital World

[www.dfes.gov.uk/byronreview/](http://www.dfes.gov.uk/byronreview/)

Care for the family

[www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf](http://www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf)

Childnet International "Know It All" CD

<http://publications.teachernet.gov.uk>

Family Online Safe Institute

[www.fosi.org](http://www.fosi.org)

Internet Watch Foundation

[www.iwf.org.uk](http://www.iwf.org.uk)

Kent leaflet for parents: Children, ICT & e-Safety

[www.kented.org.uk/ngfl/ict/safety.htm](http://www.kented.org.uk/ngfl/ict/safety.htm)

Parents Centre

[www.parentscentre.gov.uk](http://www.parentscentre.gov.uk)

Internet Safety Zone

[www.internetsafetyzone.com](http://www.internetsafetyzone.com)

Vodafone digital parenting

<http://www.vodafone.com/content/parents.html><http://www.vodafone.com/content/parents.html>

NSPCC - Share Aware

<https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware>

Parent Zone

<http://www.theparentzone.co.uk/school>

Signed by:



\_\_\_\_\_ Headteacher

Date 18.10.19



\_\_\_\_\_ Chair of Governors

Date 18.10.19