

Our Lady and St Joseph Brooms RCVA Primary School



ONLINE SAFETY POLICY

January 2021

Governors of Our Lady and St Joseph's Brooms RCVA Primary School have approved this core Online Safety Policy which will be used to educate and protect students.

ONLINE SAFETY

Online Safety encompasses the use of new technologies, internet and electronic communications, publishing and the appropriate use of personal data. It highlights the need to educate staff and pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The safe and effective use of the Internet is an essential life-skill, required by all. However, unmediated Internet access brings with it the possibility of placing users in embarrassing, inappropriate and even dangerous situations.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for children. In addition, there is information on weapons, crime and racism, access to which would be more restricted elsewhere. Children and young people must also learn that publishing personal information could compromise their security and that of others.

The previous Internet Policy has been extensively revised and renamed as the Schools' Online Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The school's Online Safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

END TO END ONLINE SAFETY

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of Online Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Durham LA including the effective management of the provided Smoothwall filtering.

SCHOOL ONLINE SAFETY POLICY

1.1 Writing and reviewing the Online Safety policy

The Online Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- The school Online Safety coordinator role is part of the Child Protection and Safeguarding roles of Key Members of the Leadership Team.

- Our Online Safety Policy has been written by the school, building on government guidance. It has been agreed by senior management and approved by Governors.
- The Online Safety Policy and its implementation will be reviewed annually.
- The Online Safety Policy was revised by: Andrew Freeman (Director of ICT Services c/o: St Bede's Catholic School & Sixth Form College)
- It was approved by the Governors: September 2017

1.2 TEACHING AND LEARNING

1.2.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.2.2 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Levels of access will vary depending on the Key Stage of the students.
- 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.

1.2.3 Pupils will be taught how to evaluate Internet content

- As a school we should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

1.3 MANAGING INTERNET ACCESS

1.3.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be implemented as part of the Schools ICT Security policy.
- Users are responsible for their own logon details and should reset passwords if they believe their account has been compromised at the earliest opportunity. Staff logon details are automatically requested to be changed on a termly basis.

1.3.2 E-mail

- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

1.3.3 Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

1.3.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents.

1.3.5 Social networking and personal publishing

- School will block/filter access to social networking sites both on Networked PC's and via the Schools wireless for all students.
- 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 or their location.
- Pupils must not place photos of other students on any social network space without explicit permission.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Regular Facebook safety sessions will be held for Students and Parents including information how to protect your social presence.
- Students are reminded that social network sites, have a minimum age restriction. For example, Facebook is 13 years of age.

- Staff are permitted to post photographs of students on the schools official social media platforms, using school devices only. Staff should not use their personal devices for the uploading.

1.3.6 Managing filtering

- If staff or pupils discover an unsuitable site, it must be reported to a member of BITS who provides the school with a managed ICT support contract.
- The BITS onsite weekly engineer will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.3.7 Managing videoconferencing

- Pupils should ask permission from the supervising teacher before making or answering a Videoconference/Skype call.
- Videoconferencing or use of Skype content will be appropriately supervised for the pupils' age.

1.3.8 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.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

1.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

1.4 POLICY DECISIONS

1.4.1 Authorising Internet access

- All staff must read and sign the 'Staff Acceptable Usage Policy before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Students must apply for Internet access individually by agreeing to comply with the Acceptable Use Policy upon logon to the System. Parents will be asked to sign and return a consent form at the start of the academic year.

1.4.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked 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.
- The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

1.4.3 Handling Online 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.
- Complaints of a Child Protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure via the schools website and upon request.
- Discussions will be held with the Police and Durham LA Safeguarding team to establish procedures for handling potentially illegal issues.

1.5 COMMUNICATIONS POLICY

1.5.1 Introducing the Online Safety policy to pupils

- Online Safety rules will be posted in all rooms and referred to on a regular basis.
- Pupils will be informed that network and Internet use will be monitored.

1.5.2 Staff and the Online Safety policy

- All staff will be given the School Online Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use have clear procedures for reporting issues.

1.5.3 Enlisting parents' support

- ☐ Parents' attention will be drawn to the School Online Safety Policy in newsletters and on the school Web site.