St. Robert's Catholic First School and Nursery

Oldgate, Morpeth, Northumberland NE61 1QF

We care, we serve, we learn together in the love and truth of Jesus

E-Safety Policy

Date Reviewed:	Review Date:
September 2022	September 2024
David Sutcliffe	Fiona Swift
Headteacher:	Chair of Governors:

School e-Safety Policy

Contents:

Importance of the Internet in School

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21 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.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

How the Internet benefits education?

The benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the LA virtual learning platform.
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the LA.
- mentoring of pupils and provide peer support for them and teachers.

How Internet use enhances learning?

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

- Staff guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.

How is e-mail managed?

- Staff e-mail is managed through the Northumberland secure portal service.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted.
- Any e-mails sent outside of the organisation come with a warning from google.
- Any sharing of personal information will be done via a secure email system such as Egress.
- The forwarding of chain letters is not permitted.
- Pupil access emails via the school360 application and is monitored by NCC.

How will published content be managed?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- The school has a Twitter/Youtube account managed by the Headteacher and an Instagram account managed by the Art lead.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.

- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, harmful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

How is Internet access authorised?

- All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.
- All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- Parents are asked to read and discuss the schools e-Safety rules with their children before access to the school systems is granted.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

How are the risks assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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. Neither the school nor NCC can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The headteacher will ensure that the e-Safety policy is implemented and

compliance with the policy monitored.

How is filtering managed?

- Despite careful design, filtering systems cannot be completely effective due to the speed of change of Web content. Filtering is performed at both the ISP and the school (Smoothwall) and ICT North (school external Technology Support company)
- SENSO Alerting security software monitors the internet usage of pupils and staff and reports any activity that is deemed unsuitable. This produces a report which is viewed by the school's IT technicians and Head Teacher.
- This monitoring will also automatically occur if the device is used at home. Any use at home which does not comply with the security in school will be flagged in the SENSO Alerting report. This will continue until the device is no longer required, when the monitoring and filtering software will be removed.
- The school will work in partnership with parents, the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the e-Safety coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the E-Safety Co-ordinator. Any requests for a website to be unblocked should be made via the school's helpdesk. The request will be assessed by a member of the e-Safety committee.

How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use Policy.

How staff are consulted?

- All staff must accept the terms of the 'Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct' statement before using any Internet resource in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and Internet and

E-mail Code of Practice and their importance explained.

- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.
- Staff development in safe and responsible Internet use, and on the school Internet policy will be provided as required.

How is our ICT system security maintained?

- The school ICT systems will be reviewed regularly with regard to

security.

- Virus protection is installed and updated regularly.
- Personal data sent over the Internet will be encrypted.
- Portable media may not be brought into school without specific permission and a virus check.
- Files held on the school's network will be regularly checked.

e-Safety - Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co- ordinator in this school is Jennifer Sykes, Deputy Headteacher. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Northumberland LA, CEOP (Child Exploitation and Online Protection) ,Childnet and Project Evolve.

Senior Management and Governors are updated by the E-Safety Co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

e-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the pupils on a regular and

meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety.

- The school has a framework for teaching internet skills in lessons based upon the National Curriculum and the framework for internet safety's (UKCIS) 'Education for a connected world' and the diocesan framework for PSHE.
- The school provides opportunities within a range of curriculum areas to teach about e-Safety based upon CEOP guidance which covers KS1, KS2 and information for parents, which can be found at www.thinkuknow.co.uk
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum
- Pupils have an age appropriate awareness of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the computing curriculum

eSafety Skills Development for Staff

- Our staff receive regular information and training on e-Safety issues in the form of staff briefings
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e- Safety and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas

Managing the School e-Safety Messages

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used
- The e-Safety policy will be introduced to the pupils at the start of each school year

- e-Safety posters will be prominently displayed

How will complaints regarding e-Safety be handled?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Any complaint about staff misuse must be referred to the headteacher.
- Responsibility for handling incidents will be delegated by the HT to a senior member of staff.
- As with drugs issues, there may be occasions when the police or child protection staff must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Sanctions available include:

➢ interview/counselling by appointed staff;
➢ informing parents or carers;
➢ removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system.
➢ other sanctions as defined in school disciplinary system.

How will Cyberbullying be managed?

- 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 school's policy on anti-bullying and in the behaviour policy.
- 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.

- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

Sanctions for those involved in cyberbullying may include:

➢ The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses

or is unable to delete content.

- ➢ Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- ➢ Parent/carers of pupils will be informed.
- ➢ The Police will be contacted if a criminal offence is suspected.

How is parents' support enlisted?

- Parents' attention will be drawn to the School Internet Policy in newsletters, the school brochure and on the school website.
- Parents are asked to read and discuss the schools e-Safety rules with their children before access to the school systems is granted.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.