St Bede's
Roman Catholic High School

ONLINE SAFETY POLICY

Scope

This policy applies to all members of the St Bede's RC High School community (staff, students, volunteers, parents, governors, and the wider community) who have access to and use the school's digital technology facilities, whether on-site or as a remote user.

This policy should be read alongside the Safeguarding & Child Protection Policy and reflects current statutory guidance, including:

- Keeping Children Safe in Education KCSIE 2026
- Working Together to Safeguard Children 2026
- UK Online Safety Act 2023

The Education and Inspections Act 2006 empowers Headteachers/Principals to such an extent that it is reasonable to regulate students' behaviour when they are off the school site and to impose disciplinary penalties for inappropriate behaviour. This includes incidents of cyber-bullying or other online safety incidents which may take place outside school but are linked to membership of the school.

The Education Act 2011 increased the powers to search electronic devices and deleted data. Action can only be taken over issues covered by the published Behaviour Policy.

Online safety is recognised as a safeguarding matter and is approached in line with the school's safeguarding procedures.

Roles and Responsibilities

Every adult member of the school community who has responsibility for the welfare of students has a responsibility to keep them safe in their use of ICT and digital technologies, including emerging technologies.

Governing Body

The Governing Body is responsible for:

- Approving the Online Safety Policy
- Reviewing and monitoring the effectiveness of the policy
- Ensuring appropriate filtering and monitoring systems are in place and regularly reviewed in line with current DfE guidance
- Reviewing the effectiveness of filtering and monitoring systems at least annually and ensuring they are appropriate to the age range, risk profile, and safeguarding needs of students.

Headteacher and Leadership Team

The Headteacher is responsible for ensuring the safety (including online safety) of all members of the School community. The day-to-day responsibility will be delegated to the online safety officer.

● The Headteacher and other designated members of the Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff

● The Headteacher/Leadership Team are responsible for ensuring that the online safety officer and other relevant members of staff receive suitable training to carry out their duties

● The Headteacher/Leadership Team will ensure that there is a system for monitoring and supporting those in school who carry out internal online safety monitoring. This is to provide a safety net and to support those who take on monitoring roles

Online Safety Officer

The Online Safety Officer:

- Take day-to-day responsibility for online safety issues
- Review online safety policies and documentation
- Ensure staff understand procedures for responding to incidents
- Provide training, advice and guidance
- Liaise with the Local Authority and relevant external agencies such as UK Safer Internet Centre (SIC) **or** Ofsted online safety
- Liaise with ICT technical staff
- Receive and log online safety incidents to inform future policy developments.
- Report regularly to the Leadership Team
- Monitor emerging online risks, including sextortion, online exploitation, harmful sexual behaviour, AI-generated content and misinformation

Network Manager / Technical Support Staff

The Network Manager and technical support team are responsible for ensuring:

- The network infrastructure is secure and protected from malicious attacks
- The school meets current online safety technical requirements, including DfE filtering and monitoring standards for schools 2026
- Secure password protection is enforced
- Filtering policies are applied and regularly updated
- Monitoring systems are implemented and updated
- Network, internet and cloud-based systems are regularly monitored
- Users are aware that monitoring takes place in line with safeguarding responsibilities

Teaching and Support Staff

Staff are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and current policy
- They have read, understood and signed the Staff Acceptable Use Policy
- Any suspected misuse or concern is reported to the online safety officer.
- Digital communication with students and parents is professional and conducted only through official school systems
- Online safety is embedded across the curriculum and other activities.
- Students understand and follow the online safety and acceptable use policies
- Students understand research skills, plagiarism and copyright.
- Student use of digital technologies is appropriately supervised

Child Protection Officer / Safeguarding Team

The Safeguarding Team should be trained in online safety issues and aware of potential safeguarding risks, including:

- Sharing of personal data
- Access to illegal or inappropriate materials
- Inappropriate online communication with adults or strangers
- Grooming
- Cyber-bullying
- Sextortion
- Online radicalisation
- AI-generated exploitation or abuse material

Students

Students are responsible for:

- Using digital technology in accordance with the Student Acceptable Use Policy
- Understanding research skills and copyright requirements
- Reporting abuse, misuse or inappropriate content
- Following policies regarding mobile devices and image use
- Applying safe online behaviour both in and out of school
- Being clearly informed about how to report online safety concerns, both within school and through external reporting mechanisms where appropriate.

Parents / Carers

Parents and carers play a vital role in supporting safe and responsible internet use.

The school will take every opportunity to help parents understand these issues through parents' evenings, letters, website and information about online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practices and to follow guidelines on the appropriate use of the internet.

● Digital video and images taken at school events

● Access to parents' sections of the website and online student data

● Their children's personal devices (such as mobile phones) in the school, where this is allowed

---

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the school's online safety provision. Children and young people need the school's help and support to recognise and avoid online risks and to build their resilience.

Online safety should be a focus in all areas of the curriculum, and staff should reinforce these messages throughout the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways: (statements will need to be adapted, depending on school/academy structure and the age of the students/pupils)

Online safety education will be delivered through:

● A planned online safety curriculum should be provided as part of Computing/PHSE and other lessons, and should be regularly revisited

● Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities

● Students/pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.

● Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

● Students/pupils should be helped to understand the need for the student/pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school

● Staff should act as good role models in their use of digital technologies, the internet, and mobile devices

● In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

● Where students are allowed to search the internet freely, staff should be vigilant in monitoring the content of the websites the young people visit.

● It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or another relevant designated person) temporarily remove those sites from the filtered list for the period of the study. Any request to do so should be auditable and include clear reasons for the need.

Technical Infrastructure, Filtering and Monitoring

The school will ensure:

- Technical systems are secure
- Regular audits of safety and security take place
- Access rights are clearly defined
- Internet access is filtered
- Illegal content is blocked
- Monitoring systems are active and effective
- Clear processes exist for reporting technical incidents
- Appropriate security measures protect servers and devices
- Personal data transferred off-site is encrypted

Use of Digital Video and Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or long term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

● When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet, e.g., on social networking sites.

● In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and, in some cases, protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students/pupils in the digital / video images.

● Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; staff's personal equipment should not be used for such purposes.

● Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

● Students must not take, use, share, publish or distribute images of others without their permission

● Photographs published on the website, or elsewhere that include students, will be selected carefully and will comply with good practice guidance on the use of such images.

● Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

● Written permission from parents or carers will be obtained before photographs of students are published on the school website. This does not have to be for each occasion, but a signed permission as the pupil starts school.

● Student's work can only be published with the permission of the student.

Data Protection

Personal data will be recorded, processed and stored in accordance with the Data Protection Act 2018.

Personal data must be:

- Processed lawfully, fairly and transparently
- Collected for specified purposes
- Adequate, relevant and limited
- Accurate and kept up to date
- Kept no longer than is necessary
- Processed securely

The school will:

- Maintain a Data Protection Policy
- Be registered with the Information Commissioner's Office
- Appoint a Data Protection Officer
- Conduct risk assessments
- Implement data breach reporting procedures

- Ensure cloud storage complies with ICO guidance

Staff must safeguard personal data and report any suspected data breach immediately.

Communication Technologies

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the school considers the following as good practice:

● The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when on school premises or using school systems (e.g., via remote access).

● Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

● Any digital communication between staff and students or parents/carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

● Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to address inappropriate communication and reminded to communicate appropriately when using digital technologies.

● Personal information should not be posted on the school website, and only official email addresses should be used to identify members of staff.

Social Media

Staff must ensure that:

● No reference should be made in social media to students, 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 the risk of loss of personal information.

Staff use of social media for educational purposes must comply with the social media policy.

Educational use of social media must comply with school policy.

Responding to Incidents

All online safety incidents must be:

- Reported immediately to the Designated Safeguarding Lead
- Logged in accordance with safeguarding procedures
- Managed in line with the Safeguarding Policy
- Low-level online concerns will also be recorded and monitored to identify patterns of behaviour and enable early intervention where appropriate.

Illegal Incidents

If there is suspicion that a website or device contains child abuse material, terrorist content or other illegal material:

- Do not investigate further
- Secure the device if appropriate
- Report immediately to the Designated Safeguarding Lead
- The DSL will refer to the police as required

Approved by: P. Crewe Name: Paul Crewe

Chair of Governors

Date: 25/03/26