St Bede's Catholic High School

E-Safety Policy

Review date: **March 2023**

Next review date: **March 2024**

Reviewed by: **Mr M Hefferan**

Approved by FGB:

E-Safety Policy

Rationale

As part of our safeguarding arrangements, we need to ensure that all Pupils access and use the internet safely and that we take all the necessary precautions to ensure this happens.

Our e-Safety Policy has been written by the school, following government guidance. It has been approved by governors.

- Pupils must have returned the parental permission form for internet use prior to receiving access
- All Pupils must read and conform to the Student Acceptable Internet Use statement
- E-safety guidelines will be posted in all ICT resource rooms and discussed with the Pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

Purpose

Teaching and Learning

Why Internet use is important?

- 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.
- The Internet is an essential element in 21st century life for education, business, and social interaction. The school has a duty to provide Pupils 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.

Internet use will enhance learning

- The school Internet access is designed expressly for Pupil use and includes filtering appropriate to the age of Pupils.
- Access to the service should not be taken up without a member of staff present.
- 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.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and 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.

Implementation

Managing Internet Access

Information system security

- School ICT systems will be reviewed regularly with regards to security.
- Virus protection is installed on all school devices and updated regularly.
- Executable files will not be allowed in Pupils' work areas or attached to e-mail
- Security strategies will be discussed with outside providers as necessary.

E-mail

- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone.
- E-mail sent to an external organization should be written carefully in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Personal email or messaging between staff and Pupils should not take place.

School web site

- The contact details on the Web site should be the school address, e-mail, and telephone number. Personal information will not be published.

Publishing Pupil's images and work

- Pupils' full names will not be used anywhere on the Web site, Newsletter or Social media, 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.
- Pupil's work can only be published with the permission of the Pupil and parents.

Social networking, chat, and instant messaging

- The school will block/filter access to social networking sites for all pupils.
- Pupils will not be allowed access to public or unregulated chat rooms.
- Any form of bullying or harassment is strictly forbidden, please refer to the school Antibullying policy
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- The dangers of using social networking sites outside of school will be expressed to both parents and Pupils.

Photographic, video and audio technology

- Pupils should always seek the permission of their teacher before making audio or video recordings within school.
- The unauthorized downloading of audio or video files is not permitted.
- Pupils must not take photos of staff members with Permission from the member of staff.

Managing filtering

- The school will work with our ISP provider to ensure systems to protect Pupils

are reviewed and improved.

- If Pupils discover an unsuitable site, it must be reported to the class teacher who will report it to IT support.
- The Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective, and reasonable.

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.
- Unauthorized use of smart devices such as mobile phones, tablets and smart watches are not to be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Mobile phone cameras should not be used, and photographs should not be forwarded or uploaded.

Protecting personal data

- Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 2018 and GDPR regulations.

Monitoring and Evaluation

Assessing risks

- The e-Safety Policy and its implementation will be reviewed annually.
- The school will keep a record of any Pupil that is restricted from the internet. The record will be kept up to date.
- 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 St. Bede's High School nor Lancashire Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.
- E-safety guidelines will be posted in all ICT resource rooms and discussed with the Pupils at the start of each year.

Handling E-Safety complaints

- Complaints of Internet misuse will be dealt with by a member of the Senior Leadership Team.
- Any complaint about staff misuse must be referred to the Headteacher.
- Discussions may be held with local police liaison officers to establish procedures for handling potentially illegal issues.
- Pupils and parents should be aware that the possession of certain types of unsuitable material or the transmission of offensive or abusive material via email or any other means may lead to prosecution by the police.

Failure to Comply

Failure to comply with the above policy will result in one or more of the following:

-

- A ban, temporary or permanent, on the use of the ICT facilities at school.
- A letter informing parents of the nature and breach of rules.
- Appropriate sanctions and restrictions placed on access to school facilities.
- Any other action decided by the Headteacher and Governors of St. Bede's High School.