St Bede's Catholic College

E-Safety Policy

St Bede's Catholic College E-Safety Policy

St Bede's staff must demonstrate that they have provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce the adverse risks of Information Communication Technology (ICT). The e-safety policy that follows explains how St Bede's intends to do this, while also addressing wider educational issues in order to help our pupils and their parents to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Education – Pupils

Whilst innovative technologies are very important, their use must be balanced by educating pupils to take a responsible approach to technology. The education of pupils in e-safety is therefore an essential part of the college's e-safety provision. Pupils need the help and support of the college to recognise and avoid e-safety risks and to build resilience.

E-Safety education will be provided in the following ways

- A planned e-safety programme is provided as part of ICT & PHSE and is regularly revisited – this covers both the use of ICT and new technologies in and outside the college
- Key e-safety messages are reinforced through displays, assemblies and planned events throughout the year.
- Pupils are helped to understand the need for the pupil Acceptable Use IT Policy (APU) by tutors & their ICT teachers.
- All staff encourage pupils to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside college
- In all lessons it is the expectation that:
  - Staff monitor the content of the websites the young people visit. Pupils are guided to sites checked as suitable for their use. The college has web filtering in place to block most unsuitable material on the web and Impero classroom monitoring software is used to allow staff to monitor & control Internet access.
  - Pupils are encouraged to be critically aware of the content they access on-line and how to to validate the accuracy of information
  - Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed online
  - Where email is being used, pupils are taught about email safety issues, such as the risks attached to the disclosure of personal details. They are taught strategies to deal with inappropriate emails and are reminded of the need to write emails clearly and correctly and not include unsuitable or abusive material.
  - The college email system is designed for schools. It has safety features in place and the capacity for Teachers to monitor email communications.
  - When using digital images, staff inform pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
- Rules for use of ICT systems are posted in all ICT rooms
- Staff are encouraged to act as good role models in their use of ICT, the internet and mobile devices
- Regular pupil surveys monitor safe usage and identify emerging trends and gaps in our e-safety education provision.
- The college website contains an e-safety information page that is regularly updated with advice for pupils on e-safety and cyberbullying.

Sexting Guidelines

Sexting is inappropriate and unsafe behaviour which threatens the social, emotional and/or physical safety of students. It can be defined as Images or videos generated by children under the age of 18, or of children under the age of 18 that are of a sexual nature or are indecent. Material is usually sent from mobile devices, via social networking or instant messaging services.

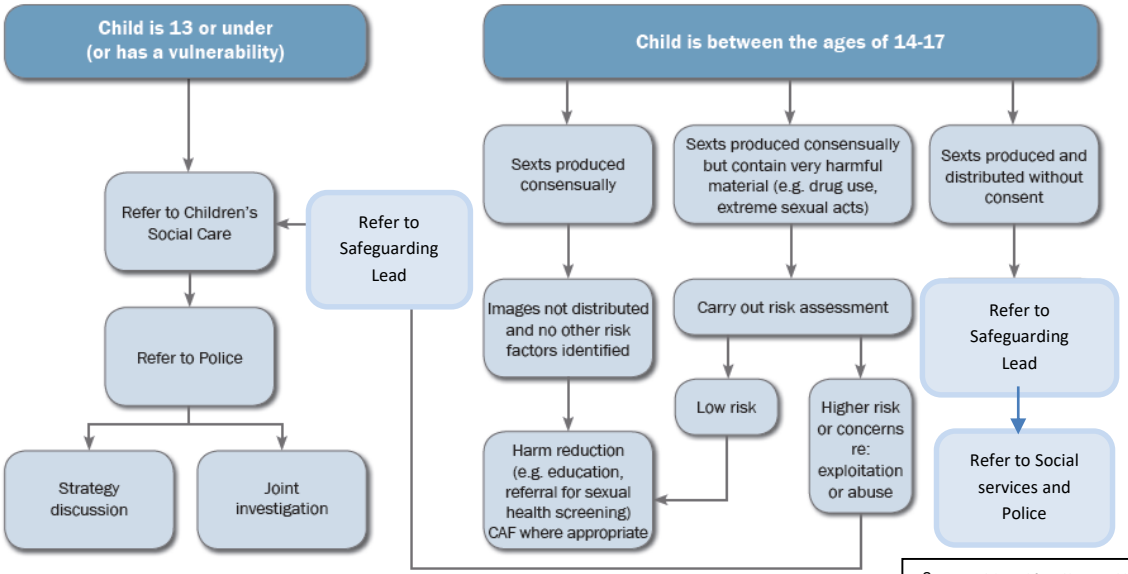
Sexting can result in humiliation, bullying and harassment of students. It is our responsibility to help to prevent sexting and the dissemination of inappropriate or offensive material. We must help young people to clearly understand both the legal and the social dangers of sexting.

Sexting and the Law : Creation, possession, advertising and distribution

Young people involved in sharing sexual videos and pictures may be committing a criminal offence. Specifically, crimes involving indecent photographs (including pseudo images) of a person under 18 years of age fall under Section 1 of the Protection of Children Act 1978 and Section 160 Criminal Justice Act 1988. Under this legislation it is a crime to:

- take an indecent photograph or allow an indecent photograph to be taken
- make an indecent photograph (this includes downloading or opening an image)
- distribute or show indecent images
- possess with the intention of distributing indecent images
- advertise indecent images
- possess indecent images.

Sexting incidents – The chart below outlines the procedure to follow if Sexting is discovered that involves a pupil at St. Bede's Catholic College;



Source : *Adapted from Naace guidance for schools on Sexting 2012*

Education – parents

The college provides information to parents and carers through:

- A Year 7 parents e-safety evening
- E-safety tips in the college newsletter every two weeks
- The school website contains an e-safety information page that is regularly updated with advice for parents on e-safety and cyberbullying

Training – Staff

Training is offered as follows:

- A planned programme of formal e-safety training is delivered to all new staff as part of the induction programme.
- All staff receive regular advice, guidance and training from the E-Safety Coordinators through staff meetings, Inservice training, memos & emails.
- Through the college appraisal process, staff can identify e-safety as a training need and this will be responded to as appropriate.
- All staff are required to read and sign the college Acceptable Use Policy.
- The E-Safety Coordinators receive regular updates through attendance at training sessions and by reviewing guidance documents released.

Training – Governors

Governors receive guidance on e-safety and receive relevant updates on issues as they emerge.

- Training is provided as and when required.
- Information on sessions run for staff or parents.

Technical

The college network manager is responsible for ensuring that the college infrastructure and networks are as safe and secure as is reasonably possible.

- Users are responsible for the security of their network accounts.
- Username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The college maintains and supports a managed filtering service
- Requests from staff for sites to be unblocked must be made direct to the Network Manager
- College ICT technical staff regularly monitor the activity of users on the college ICT systems and report concerns to the Vice Principal
- An appropriate system is in place (emailing the ICT help desk) for users to report any actual or potential e-safety incident to the Network Manager
- Remote classroom management tools are used by staff to control pupil's workstations and view their activity

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. This states that personal data must be fairly and lawfully processed, processed for limited purposes, relevant, not excessive, accurate, kept no longer than is necessary, processed in accordance with the data subject's rights, secure and only transferred to others with adequate protection.

Staff must ensure that they:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption or secure password protected devices and documents.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies the college considers the following as good practice:

- When dealing directly with college business, staff use only the college email (@stbcc.org) service to communicate with other staff, other professionals, pupils and parents
- Staff should not use personal email accounts for college business
- Email communications may be monitored
- Staff must report to their line manager the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents must be professional in tone and content.
- Personal email addresses, text messaging or public chat and social networking programmes must not be used for communications with pupils or parents about their children.

This Policy has been drawn up following consultation and should be read in conjunction with the Safeguarding Policy and Acceptable Use Policies for pupils and staff.

This policy will be reviewed on an annual basis.

Acknowledgements:

We would like to acknowledge the following organisations whose policies, documents, advice and guidance have contributed to the development of this E-Safety Policy:

SWGFL – South West Grid for Learning

RM Education – E-Safety. A practical guide for schools.