



E-SAFETY POLICY

E-Safety Policy

Scope

This policy applies to all members of St Bede's RC High school community (staff, students, volunteers, parents, governors, wider community) who have access to and use the school's ICT facilities either onsite or as a remote user.

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school / academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school / academy, but is linked to membership of the school / academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Roles and Responsibilities

Every adult member of the school community who has a responsibility towards the welfare of the students has a responsibility towards keeping the students safe in their use of ICT. This section outlines the different responsibilities of the different groups and individuals

Governing Body

The Governing body are responsible for the approval of the E-Safety policy and reviewing and monitoring the effectiveness of the policy.

Head Teacher & Leadership Team

- The Headteacher responsibility for ensuring the safety (including e-safety) of all members of the School community. The day to day responsibility will be delegated to the E-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 e-safety allegation being made against a member of staff
- The Headteacher/Leadership Team are responsible for ensuring that the E-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 e-safety monitoring. This is to provide a safety net and to support those who take on monitoring roles

E-Safety Officer

- Day to day responsibility for e-safety issues and has a leading role in reviewing the e-safety policies and documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident occurring
- Provides training, advice and guidance for staff

- Liaises with the Local Authority and other relevant bodies
- Liaises with the ICT technical staff
- Receives reports of and logs e-safety incidents to inform future policy developments
- Reports regularly to Leadership Team

Network Manager / Technical Support Staff

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

- That the network infrastructure is secure and is not open to malicious attacks
- The School meets the required e-safety technical requirements
- That users may only access the networks and devices through a properly enforced password protection policy in which passwords are secure
- The filtering policies are applied and regularly updated
- They keep up to date with e-safety technical information in order to effectively carry out their e-safety responsibility
- That the use of the network, Internet, CC4 Anywhere remote access and Trinity Cloud is regularly monitored in order that any misuse or attempted misuse can be reported to the E-safety officer
- That monitoring software and systems are implemented and updated

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the E-safety Officer
- All digital communication with students / parents / carers should be on a professional level and ONLY carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Students understand and follow the e-safety and acceptable use policies
- Students have a good understanding of research skills and need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies such as computers, mobile phones, cameras etc in lesson and other school activities where allowed.
- In lessons where Internet use is pre-planned 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 may be found in Internet Searches

Child Protection Officer Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- inappropriate online communication with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Students

- Students are responsible for using the digital technology in accordance with the Student Acceptable Use Policy
- Have a good understanding of research skills and need to avoid plagiarism and uphold copyright regulations
- Need to know the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices. They should also know and understand policies on the taking of and use of images and on cyber-bullying
- Should understand the importance of adopting good e-safety practices when using digital technologies out of school and realise that their actions out of school, if related to their membership of the school, are still covered by the e-safety policy.

Parents / Carers

Parents / carers play a vital role in ensuring that their children understand the need to use digital technology and the Internet in a safe and responsible way. The school will take every opportunity to help parents understand these issues through parents' evenings, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practices and to follow guidelines on the appropriate use of

- 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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-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)

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-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 on-line 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 freely search the internet, 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 other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education - Parents/carers

Some parents and carers may have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents' evenings
- High profile events / campaigns eg Safer Internet Day

Education and Training - Staff and Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Training - Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are responsible for e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical - Infrastructure, Equipment, Filtering, Monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities. This can be found in the schools Code of Conduct and the Staff Handbook.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school's technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the technical team who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every academic year.

- The “administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- The network manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. (the school / academy will need to decide on the merits of external / internal provision of the filtering service. There is a clear process in place to deal with requests for filtering changes
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed system is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- A system is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- Appropriate security is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An appropriate system is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

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 longer 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 eg 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, the personal equipment of staff 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, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:



- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”. (see Privacy Notice section in the appendix)
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner’s Office.

Staff must ensure that they:

- At all times take care to ensure the safekeeping 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 and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software

- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

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 in school, or on school systems (eg by 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 e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need 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

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school / academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should 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 risk of loss of personal information.

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

Responding to Incidents This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the Safeguarding Policy for responding to online safety incidents and report immediately to the poli