ST. BEDE'S CATHOLIC JUNIOR SCHOOL

celebrates life and learning

E-SAFETY POLICY

MISSION STATEMENT

St. Bede, patron of our school, wrote:

"It was always my delight to learn and to teach".

We are a celebrating community, living the
Gospel Values, committed to educating children
in the light of the Catholic Faith.

We journey together so that we

"Might have life - life in all its fullness".

John 10:10

RATIONALE

The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The E-safety Policy helps to ensure safe and appropriate use. The development and implementation of such a strategy involves all the stakeholders in a child's education from the Governors, Headteacher, Senior Leadership Team, classroom teachers, support staff, parents / carers, members of the community and the pupils themselves.

We recognise that there is a range of risks to young people in the digital environment. As with all risks, it is impossible to eliminate risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the digital experiences they encounter and to which they may be exposed, so that they have the confidence and skills to face and deal with these issues in an appropriate and timely manner. The E-safety Policy explains how we do this.

ROLES AND RESPONSIBILITIES

Governing Body

Governors are responsible for the approval of the E-safety Policy and for reviewing the effectiveness of the Policy. This will be carried out by the Governing Body receiving information about E-safety incidents, where appropriate.

Headteacher and Senior Leadership Team

- The Headteacher is responsible for ensuring the safety (including E-safety) of members of the school community;
- The Headteacher and Senior Leadership Team are responsible for ensuring that the E-safety Officer/ICT Subject Leader and other relevant staff receive suitable CPD to enable them to carry out their E-safety roles and to train other colleagues, as relevant;
- The Headteacher / Assistant Headteacher will seek advice from Halton LA and MGL in the event of a serious E-safety allegation being made against a member of staff;
- E-safety provision is reviewed within the School Management Plan.
- The Headteacher and Senior Leadership Team are aware of GDPR Policy (refer to GDPR Policy) and the importance of protecting the safety of data in relation to the school, its staff, pupils and wider community.

E-safety Officer/ICT Subject Leader

- Updates the Acceptable Use Policy for staff and children;
- Reviews the school E-safety Policy and associated documents;
- Ensures that all staff are aware (as part of staff induction) of the procedures that need to be followed in the event of an E-safety incident taking place;
- Attends latest training on E-safety to disseminate in school;
- Provides training and advice for staff;
- Liaises with the Local Authority;
- Liaises with school ICT technical support staff regularly;
- Meets with Computing Governor to discuss current issues;
- Attends relevant Governing Body meetings;
- Reports to Senior Leadership Team when needed.
- Is aware of GDPR Policy (refer to GDPR Policy) and the importance of protecting the safety of data in relation to the school, its staff, pupils and wider community.

Technical Support Staff

MGL ensure that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack;
- the school meets the E-safety technical requirements outlined in any relevant Local Authority E-safety Policy and guidance;
- users may only access the school's networks through a properly enforced password protection policy;
- MGL inform Headteacher and/or Designated member of SLT responsible for filtering and monitoring of issues relating to the monitoring and filtering in place;
- they keep up to date with E-safety technical information in order to effectively carry out their E-safety role and to inform and update others as relevant;

- the use of the network, website, remote access, e-mail is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher, Senior Management Team and E Safety Officer for investigation / action / sanction;
- web filtering solutions are reviewed (current system in place is E SET End Point Security);
- monitoring software / systems are implemented and updated as agreed in school policies;
- Is aware of GDPR Policy (refer to GDPR Policy) and the importance of protecting the safety of data in relation to the school, its staff, pupils and wider community.

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 school Staff Acceptable Use Policy / Agreement (AUP);
- They report any suspected misuse or problem to the E-safety Officer/ICT Subject Leader for investigation / action / sanction;
- Digital communications with pupils (e-mail / website / voice) should be on a professional level and only carried out using official school systems;
- E-safety issues are taught progressively throughout the curriculum and other school activities (school employs E Aware Safety scheme that staff has received training on and all curriculum resources are on shared drive for staff to access);
- Pupils understand and follow the school E-safety and Acceptable Use Policy;
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They monitor ICT activity in lessons, extra-curricular and extended school activities;
- They are aware of E-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices. Under no circumstances can staff use personal equipment to take images of pupils at, or on behalf of, the school;
- In lessons where Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in Internet searches;
- They have “due regard to the need to prevent people from being drawn into terrorism”. (Sections 26 and 29 Counter-Terrorism and Security Act, 2015).
- Is aware of GDPR Policy (refer to GDPR Policy) and the importance of protecting the safety of data in relation to the school, its staff, pupils and wider community.

Designated Safeguarding Lead

Is trained in E-safety issues and is aware of the potential for serious child protection issues to arise from:

- Sharing of personal data;
- Access to illegal / inappropriate materials;

- Inappropriate on-line contact with adults / strangers;
- Potential or actual incidents of grooming;
- Cyber-bullying;
- Misuse or manipulation of images for pornographic or grooming purposes.
- Is aware of GDPR Policy (refer to GDPR Policy) and the importance of protecting the safety of data in relation to the school, its staff, pupils and wider community.

Pupils

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they are expected to sign before being given access to school systems;
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Are expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They know and understand school policies on the taking / use of images and on cyber-bullying;
- Understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the school's E-safety Policy covers their actions out of school, if related to their membership of the school.
- Understand the importance of 'data', both personal and impersonal, and how to protect it and treat it with respect, reporting misuse to a member of staff.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. Parents / carers are invited to attend training and information about national / local E-safety campaigns and we also hold E-safety evenings. We have a tab on the website which is dedicated to E-safety and we also publish a monthly E-safety newsletter on the website, our Facebook Page and Twitter. Parents and carers are responsible for endorsing (by signature) the Pupil Acceptable Use Policy.

EDUCATION: PUPILS

- E-safety is integral to all Computing lessons and whenever electronic equipment is used; 're-cap' lessons are taught explicitly at the start of each new year;
- Pupils are reminded not to share personal details;
- Pupils are made aware of their digital footprint and the difficulty of removing content once it has been posted online;
- Social networking sites and their associated risks are regularly discussed with pupils and information is shared with parents / carers / pupils / staff on a monthly basis via the E-safety tab on the website (monthly newsletter);
- Pupils are taught in all lessons, where appropriate, to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information;

- Pupils are helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school;
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet;
- Pupils are taught where to seek advice or help if they experience any problems online or with related technologies; i.e. parent / carer, teacher / trusted staff member, external organisation such as Childline, CEOP;
- Staff act as good role models when using the Internet and electronic devices.

EDUCATION – PARENTS / CARERS

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

- Letters, newsletters, website, Twitter, Facebook Page;
- Child - Teacher - Parent / Carer evenings;
- Regular training and updates to help them to understand how to protect their children at home;
- Parents / Carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school;
- Parents / Carers are required to make a decision as to whether they consent to images of their child being taken / used in the school domain (e.g., on school website, Twitter page).

EDUCATION AND TRAINING – STAFF

All staff receive E-safety training and understand their responsibilities, as outlined in this Policy. Training is offered as follows:

- A planned programme of formal E-safety training is made available to staff. An audit of the E-safety training needs of all staff is carried out annually. It is expected that some staff may identify E-safety as a training need within the appraisal process;
- All new staff receive E-safety training as part of their induction programme, ensuring that they fully understand the school E-safety Policy and Acceptable Use Policies;
- The E-safety Officer receives regular updates through attendance at training sessions and by reviewing guidance documents;
- This E-safety Policy is presented to and discussed by staff in staff meetings;
- E-safety materials and resources are made available on the staff shared drive ;
- Any E-safety concerns, which are brought to light, are shared amongst staff via the Headteacher so that the issues can be addressed with a whole-school approach;
- All adults working with children are aware of how to escalate concerns regarding E-safety incidents.

TRAINING – GOVERNORS

Governors are encouraged to take part in E-safety training / awareness sessions, with particular importance for those who are members of any committee involved in ICT / E-safety / health and safety / child protection. This will 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 / carers;
- Online training, for example, Prevent / GDPR training.

TECHNICAL

Infrastructure / Equipment, Filtering and Monitoring

The school is 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 ensures that the relevant people named in the above sections will be effective in carrying out their E-safety responsibilities.

- The school ICT systems is managed in ways that ensure that the school meets the E-safety technical requirements outlined in the Halton LA Acceptable Use Policy and any relevant Local Authority E-safety documentation and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling will be securely located and physical access restricted.
- All users have clearly defined access rights to school ICT systems.
- All users are provided with a username and password by MGL.
- The school supports the managed filtering and reporting service provided by MGL.
- MGL ICT Services regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Any actual / potential E-safety incident is reported directly to the Headteacher who takes the necessary action.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software, monitoring and filtering software from MGL.
- Staff use encrypted storage devices when working on and off site.
- Staff files are saved in a shared area which is not accessible by pupils.
- Programs can only be installed by MGL.

CURRICULUM

E-safety is taught progressively throughout the curriculum and staff reinforce E-safety messages in the use of ICT across the curriculum.

- In lessons where Internet use is pre-planned, it is best practice that pupils are 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;
- The school has adopted the ‘E Aware Safety’ scheme. All curriculum resources are on the shared drive for staff to access;
- Where pupils are allowed to freely search the Internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the children visit and ensure the highest security and that the pupils are supervised at all times;
- Pupils are 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;
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet;
- Pupils are taught to be polite and respectful when communicating.

USE OF DIGITAL AND VIDEO IMAGES - PHOTOGRAPHIC, VIDEO

- When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they recognise the risks attached to publishing their own images on the Internet, e.g. on social networking sites;
- Staff 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 are only taken on school equipment, the personal equipment of staff is not used for such purposes;
- Care is taken when taking digital / video images of pupils and that images taken are selected carefully and comply with good practice guidance;
- Pupils do not take, use, share, publish or distribute images of others without their permission;
- Photographs published on the website, Twitter, or elsewhere that include pupils, are selected carefully and comply with good practice guidance on the use of such images;
- Pupils’ full names are not be used anywhere on-line, particularly in association with photographs;
- Written permission from parents / carers is obtained before photographs of pupils are taken and published on-line, or displayed in school.

GDPR

- Please refer to the GDPR Policy (Appendix I)

COMMUNICATIONS

- All staff have an @stbedesjuniorschool email address;

- Users need to be aware that e-mail communications may be monitored.
- Any digital communication and content sharing (lessons / homework for example) between staff and pupils or parents / carers (e-mail, website, home-learning platforms etc.) is professional in tone and content. These communications may only take place on official (monitored) school systems. Personal accounts must not be used for these communications.
- Pupils are taught about e-mail safety issues, such as the risks attached to the use of personal details. They learn strategies to deal with inappropriate e-mails and are reminded of the need to write e-mails clearly and correctly and not include any unsuitable or abusive material.
- Personal information is not to be posted on the school's on-line media outlets.
- The school uses the website, Twitter and a Facebook Page to share achievements and information. This is monitored by the E-safety Officer and Headteacher.

REMOTE LEARNING

During school closures, pupils are accessing remote learning platforms. Parents / carers and pupils are aware that staff has access to their online learning space and can monitor and respond to work submissions. There is also the ability to message staff members and parents / carers and pupils are encouraged to maintain a professional and appropriate dialogue throughout.

Staff is aware of using professional language in all digital communications and using online learning platforms appropriately to create, share and respond to remote learning in addition to disseminating homework tasks.

Regular E Safety information has been shared with the school community throughout school closures and can be found on the school's E Safety tab on the website, the School's Computing Curriculum Page, Facebook Page and Twitter account.

RESPONDING TO INCIDENTS OF MISUSE

In the event of such a situation arising, it will be dealt with in accordance with school policy. In the event of a serious infringement, advice will be taken from MGL, Halton LA and any other relevant organisations. It is recommended that legal advice is sought in the event of an E-safety issue or situation.

PREVENT DUTY

All staff has been trained to ensure that pupils are safe from terrorist and extremist material when accessing the Internet in school. The LA's filtering system monitors access to inappropriate sites and children are supervised when using the Internet.

The contact information for Cheshire Constabulary Prevent and Channel Team are as follows:

Team email: prevent@cheshire.pnn.police.uk

REVIEW

The E-safety Policy is a working document. It will be reviewed in the light of training and changes in legislation. Any amendments will be agreed by the staff and Governing Body.