St Bede’s School

E-Safety Policy

Purpose of the Policy

- St Bede’s School recognises that ICT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge pupils, and support creativity and independence.
- Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that pupils, staff and parents use it appropriately and practice good e-safety.
- It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.
- E-safety covers the internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.
- There is a ‘duty of care’ for any persons working with children and educating all members of the school community on the risks and responsibilities of e-safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential.
- This policy aims to be an aid in regulating ICT activity in school, and provide understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.
- Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures. With due regard to Keeping Children Safe in Education (May/September 2016), these protocols can be found in section 7 of the Anti-bulling Policy and under section 1.7 (Peer on peer abuse) of the Safeguarding Policy. Staff undergo regularly updated safeguarding training which includes online safety.

1. Roles and responsibility

1.1 The person accountable for e-safety is the Headmaster, Mr Charlie.

1.2 The person responsible for pupil awareness is the IT teacher, Mrs Wheat

1.3 The person responsible for safeguarding is the DSL, Mr Platts

1.4 All employees are responsible for adherence to the Policy for Safeguarding and related procedures regarding any use of mobile phones, cameras and recording devices.

2. Communicating school policy

2.1 This policy is available from the school office and on the school website for parents, staff, and pupils to access when and as they wish.

2.2 Rules relating to the school code of conduct when online, and e-safety guidelines, are discussed in IT classes and signed for using the ICT User Agreement (see Appendix 1)

2.3 E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during other lessons and sessions where personal safety, responsibility, and/or development are being discussed.

3. What is an e-Safety Incident?

3.1 Given the enormous complexities of the factors that may constitute 'risk', the following classifications are helpful in providing some structure. However, it is important to remember that there is overlap between categories and boundaries are sometimes blurred.

3.2 The Proprietors will have a whole school approach to online safety, and do all they reasonably can to limit children's exposure to the risks around content, contact and conduct from the school's IT system. The age range of pupils, how often they access the school's IT system and the proportionality of costs vs risks will be considered.

3.3 In using the categories of Content, Contact and Conduct, it is possible to contextualise a definition of 'potentially harmful or inappropriate material'. It is acknowledged that in practice these provide a useful framework for 'replacing emotion with facts' when confronted with specific issues or concerns. It is also helpful to exemplify the broad range of potentially harmful or inappropriate behaviours.

3.4 CONTENT (child as recipient)

- Adverts, spam, sponsorship, personal info, violent and hateful content, pornography, unwelcome sexual content, bias, misleading information or advice

CONTACT (child as participant)

- Tracking, harvesting of personal information, being bullied, harassment, stalking, meeting strangers, being groomed, self-harm, unwelcome persuasion

CONDUCT (child as perpetrator)

- Illegal downloading, hacking, gambling, financial scams, terrorism, bullying, harassment, creating/uploading material, providing misleading information

4. Making use of ICT and the internet in school

4.1 The internet is used in school to raise educational standards, to promote pupil achievement, to support professional work of staff and to enhance the school's management functions.

4.2 Technology is advancing rapidly and now a huge part of life, education and business. We want to equip our pupils with all necessary skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

4.3 Pupil benefits include:

- Access to worldwide educational resources such as art galleries, museums and libraries, to subject experts, role models, inspirational people and organisations, providing opportunity for pupils to interact with people that they otherwise would never be able to meet. An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs. Access whenever and wherever convenient. Freedom to be creative, to explore the world and cultures from within a classroom. Social inclusion, in class and online. Access to case studies, videos and interactive media to enhance understanding. Individualised access to learning. Use of ICT.

4.4 Staff benefits include:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies. Immediate professional and personal support through networks and associations. Improved access to technical support. To track pupil's progress throughout the year.

4.5 The school has its own Wi-Fi system which is filtered, monitored and managed through school protocols. Pupils are not allowed unlimited and unrestricted access to the internet via 3G and 4G unless specific permission is sought from the Headmaster.

4.6 Children will be taught about online safety through specific modules in IT sessions, as well as in general teaching using IT equipment and lessons with elements of PSHE and SRE.

5. Learning to evaluate internet content

5.1 With so much information available online it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Pupils will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate to use age-appropriate tools to search for information online to acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Pupils who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

5.2 The school filters internet content to ensure that it is appropriate to the age and maturity of pupils. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate personnel. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

- The appropriateness of filtering and monitoring systems will be informed by the assessment of risk, including the Prevent Duty.

6. Managing information systems

6.1 The school is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal protection of our community very seriously. The security of school information systems and users will be reviewed by the Headmaster and virus protection software will be updated.

7. Emails

7.1 The school uses email for contacting parents as part of school communication. Staff should not use an email address to contact parents unless permission sought from the Headmaster.

7.2 Staff and pupils are aware that school email accounts are only used for school matters.

7.3 Emails sent from school accounts should be carefully written. Staff are representing the school and should take this into account when entering into any email communications.

7.4 Staff must tell a member of the SMT if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves. The forwarding of chain messages is not permitted in school.

8. Published content and the school website

8.1 The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, pupils, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

8.2 The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy. No personal information on staff or pupils will be published and details for contacting the school will be for the school office only.

8.3 The website will be maintained by designated staff only via permission of the Headmaster.

9. Guidance of safe use of images of children

9.1 Photographs can bring our school to life, showcase our pupil's talents, and add interest to publications both online and in print. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

9.2 Images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs over a period of time rather than a one-off incident is more convenient for all involved.

9.3 Using images of children:

- The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.
- It is important that published images do not identify pupils or put them at risk of being identified. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children:
    - Parental consent must be obtained. Consent will cover the use of images in:
        - all school publications
        - on the school website
        - in newspapers as allowed by the school
        - in videos made by the school or in class for school projects.
- Electronic and paper images will be stored securely. Names of stored photographic files will not identify the child. Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (ie a pupil in a swimming pool, rather than standing by the side in a swimsuit). Groups may be referred to collectively by year group or form name. Events recorded by family members of the pupils such as school plays or sports days must be used for personal use only and must not be published on any social media sites.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils.
- Parents should follow the standard school complaints procedure if they have a concern/complaint regarding misuse of school photographs. Please refer to our complaints policy for more information on steps to take when making a complaint.

10. Social networking:

10.1 Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms, online gaming and instant messaging programs. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person.

10.2 It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. Social media sites have many benefits for both personal use and professional learning; however, both staff and pupils should be aware of how they present themselves online. Pupils are taught through IT and other curriculum areas as appropriate about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place.

10.3 The school follows general rules on use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.

- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Pupils and staff will not publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory.
- The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.

11. Mobile phones and personal devices

11.1 While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly.

11.2 Some issues surrounding the possession of these devices are:

- can make everyone more vulnerable to cyberbullying they can be used to access inappropriate internet material they can be a distraction in the classroom they are valuable items that could be stolen, damaged, or lost they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

11.3 The school takes certain measures to ensure that mobile phones are used responsibly in school. The school will not tolerate cyberbullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the school's disciplinary sanctions read the school behaviour policy.

11.4 Pupils are not permitted to bring mobile technology into the school, unless an agreement with the school is already in place (eg boarding pupils). No pupils are allowed mobile technology during the hours of 9am and 5pm without permission from the SMT.

11.5 Staff mobile phones must be switched off or placed in silent mode during school lessons or any other formal school activities. If staff wish to use these devices in class as part of a learning project, they must get permission from a member of the SMT.

11.6 Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school's behaviour policy. Their mobile technology will be confiscated.

11.7 Staff are not permitted to take photos or videos of pupils without permission of the SMT.

11.8 The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' whilst on duty – this includes any formal events outside of school hours. Any breach of school policy may result in disciplinary action against that member of staff.

12. EYFS specific issues

12.1 The Early Years Foundation Stage has a detailed policy regarding the 'Acceptable Use of Mobile Phones, Cameras and Recording Devices'

12.2 Please see Appendix 5 of the Policy for Safeguarding incorporating Child Protection

13. Cyberbullying

13.1 Cyberbullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the relevant policies.

13.2 The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

14. Managing emerging technologies

14.1 Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have.

14.2 The school strives to keep up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

15. Protecting personal data

15.1 St Bede's School believes that protecting privacy and regulating safety through data management, control and evaluation is vital to whole-school and individual progress.

15.2 The school collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

15.3 We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. Assessment results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and pupils.

Headmaster	Director of Studies
September 2016	September 2016

Appendix 1 - St Bede’s School ICT User Agreement

St Bede’s School

ICT User Agreement

This agreement has been drawn up to protect all parties – pupils, staff and school

ICT Equipment

- Users will not:
    - X Divulge passwords to anyone other than authorised users
    - X Allow any unauthorised person the use of ICT equipment
    - X Install/download software onto ICT equipment owned by the school
    - X Copy or delete any software from ICT equipment owned by the school
    - X Change the configuration of any ICT equipment owned by the school
    - X Attempt to access any area that has been protected
    - X Store undesirable material on any part of the school system
    - X Attempt to repair any ICT equipment owned by the school
    - X Borrow any ICT equipment without express permission
    - X Attach any peripheral to ICT equipment owned by the school
    - X Eat or drink near any ICT equipment
    - X Carry more than two iPads at a time
    - X Transport the iPad trolley without express permission
- Users will:
    - ✓ Report any accidental infringement of the above conditions
    - ✓ Treat all equipment with respect and leave work areas tidy

Internet Access

- All users of the internet are responsible for their own behaviour
- No activity performed which threatens the system’s integrity
- Users may not enter into any online contracts/agreements
- Online chat is not permitted without express permission
- Webcam use is not permitted without express permission
- Copyright of any material must be respected and valued
- Access must only be made through school ICT equipment unless express permission is granted for use of personal equipment
- Access/sending of inappropriate and offensive material is not permitted under any circumstances

I agree to all the above statements, and understand that violations will result in a temporary or permanent ban on any ICT use at St Bede’s School

Name:________________________________

Signed:_______________________________

Date:_________________________________