E Safety Policy

1 INTRODUCTION

1.2 This policy has been developed to ensure that all adults in St Bede's are working together to safeguard and promote the welfare of children and young people.

1.2 E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

1.3 This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities by using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

1.4 The Headteacher has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

1.5 This policy complements and supports other relevant school policies including Acceptable Use Agreements, anti-bullying, mobile phone, and safeguarding policies. All staff must adhere to the instructions in the Staff Handbook.

1.6 The purpose of internet use in school is to help raise educational standards, promote pupil achievement and support the professional work of staff as well as enhance the school's management information and business administration systems.

1.7 The internet is an essential element in 21st-century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience as well as education them about the responsible use of the internet and related media.

1.9 A risk assessment will be carried out before children and young people are allowed to use new technology in schools and settings.

2 ETHOS

2.1 It is the duty of the school to ensure that every child and young person in its care is safe. This applies to the 'virtual' or digital world. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

2.2 Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures.

2.3 All staff have a responsibility to support e-Safe practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols.

2.4 E-safety is a partnership concern and is not limited to school premises, school equipment or the school day.

2.5 Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will dealt with in accordance with the school's Anti-Bullying and Behaviour Policy.

2.6 Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy.

3 ROLES AND RESPONSIBILITIES

3.1 The Headteacher will ensure that:

- All staff should be included in E-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- A Designated member of Staff for E-Learning and Safety is identified and receives appropriate on-going training, support and supervision and works closely with the Designated Person for Safeguarding.
- All temporary staff and volunteers are made aware of the school's E-Learning/Safety Policy and arrangements.
- A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.

3.2. The Governing Body of the school will ensure that:

- There is an appropriate member of the school's staff who is designated to take the lead on E-Learning/Safety within the school.
- Procedures are in place for dealing with breaches of e-safety and security.
- All staff and volunteers have access to appropriate ICT training.

3.3 The Designated member of staff for E-Learning/Safety will:

- Act as the first point of contact with regards to breaches in e-safety and security.
- Liaise with the Designated Person for Safeguarding as appropriate.
- Advise the headteacher on ICT security so that it is fit for purpose.
- Attend appropriate training.
- Provide support and training for staff and volunteers on E-Safety.
- Update the school's Acceptable Use Agreement as required
- Ensure that all staff and volunteers understand and aware of the school's E-Learning/ Safety Policy.
- Liaise with the School technical staff to ensure that the school's ICT systems are regularly reviewed with regard to security.
- Liaise with the School technical staff to ensure that the virus protection is regularly reviewed and updated.
- Liaise with the Headteacher to ensure the school monitoring software (Securus) is fit for purpose

4 TEACHING and LEARNING

Benefits of internet use for education

4.1 The internet is a part of the statutory curriculum and a necessary tool for staff and children and young people and benefits education by allowing access to worldwide educational resources and enabling access to specialists in many fields.

4.2 Access to the internet supports educational and cultural exchanges between students worldwide, and enables pupils to participate in cultural, vocational, social and leisure use in libraries, clubs and at home.

4.3 The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data with the Local Authority and DfE.

4.4 The internet improves access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, government initiatives.

4.5 The internet offers opportunities for mentoring pupils and providing peer support for them and their teachers.

4.6 Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of the children and young people.

4.7 Children and young people will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

4.8 Children and young people will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information. Children and young people will also be taught that copying material is worth little without an appropriate commentary demonstrating the selectivity used and evaluating the material's significance.

4.9 Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

5 MANAGING INTERNET ACCESS

5.1 Developing good practice in internet use as a tool for teaching and learning is essential. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children and young people.

5.2 Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide pupils in online activities that will support the learning outcomes planned for the pupil's age and maturity.

5.3 Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

5.4 If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Co-ordinator.

5.5 The school will ensure that the use of internet-derived materials by staff and pupils complies with copyright law.

5.6 Pupils will be taught to be critically aware of the materials they read as well as how to validate information before accepting its validity.

6 MANAGING EMAIL

6.1 Personal email or messaging between staff and pupils should not take place. This should be clarified to "Personal email or messaging between staff and pupils should not take place. Staff should not share their private email addresses with students. Email conversations should never be of a personal nature."

6.2 Staff must use the school email address if they need to communicate with pupils about their school work e.g. study leave, course work etc.

6.3 Pupils and staff may only use approved email accounts on the school system and pupils must inform a member of staff immediately if they receive an offensive email. 6.4 Pupils must not reveal details of themselves or others in any email communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.

6.4 Access in school to external personal email accounts may be blocked.

6.5 Excessive social email use can interfere with learning and will be restricted.

6.6 Email should be authorised before sending to an external organisation just as a letter written on school headed note-paper would be.

6.7 The forwarding of chain letters is not permitted.

6.8 Incoming email should be monitored and attachments should not be opened unless the author is known.

7 MANAGING WEBSITE CONTENT

7.1 Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

7.2 Photographs of pupils will not be used without the written consent of the pupil's parents/carers.

7.3 The point of contact on the school website will be the school address, school email and telephone number. Staff or pupils' home information will not be published.

7.4 The headteacher or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate.

7.5 The website will comply with the school's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing.

7.6 The names of pupils will not be used on the website without their permission. Where photographs of students are used it is good practice not to add the students name beside the photograph though it could be mentioned elsewhere on the website.

7.7 Work will only be used on the website with the permission of the pupil and their parents/carers.

7.8 The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

7.9 Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

8 SOCIAL NETWORKING AND CHAT ROOMS

8.1 The school will control access to moderated social networking sites and educate pupils in their safe use.

8.2 Pupils will not access social networking sites whilst at school.

8.3 Pupils will be taught the importance of personal safety when using social networking sites and chat rooms.

8.4 Pupils will not be allowed to access public or unregulated chat rooms.

8.5 Pupils will only be allowed to use regulated educational chat environments and use will be supervised.

8.6 Newsgroups will be blocked unless an educational need can be demonstrated.

8.7 Pupils will be advised to use nick names and avatars when using social networking sites.

8.8 Staff will not exchange social networking addresses or use social networking sites to communicate with pupils.

8.9 Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a pupil is necessary, the agreement of a senior manager should always be sought first and language should always be appropriate and professional.

8.10 Staff are required to follow the school's social media policy.

9 MOBILE PHONES

9.1 The school has a separate policy on the use of mile phones by pupils in school. Staff should not use their own mobile phone in lesson or in public areas, except in exceptional circumstances

9.2 Use of cameras on their mobile phones by pupils will be kept under review will only be permitted under the close supervision of a teacher (for example to photograph art work).

9.3 Staff will be issued with a school mobile phone where contact with pupils is necessary.

9.4 Where mobile phones/tablets are used to photograph school activities they will only be for use in school, permission of the child will be obtained (except for looked after children) and the image will be permanently deleted from the device as soon as possible.

10 FILTERING

10.1 . The school will work in partnership with parents/carers, the Local Authority, the DfE and the Web Filtering Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly

10.2 If staff or pupils discover unsuitable sites, the URL (address) and content must be reported and the member of staff with responsibility for E Safety who will contact the IT technician to block the content**.**

10.3 Any material the school deems to be under the remit of the Internet Watch Foundation www.iwf.org.uk<http://www.iwf.org.uk> (illegal sexual content) should be immediately referred to them via the DSL. All other unsuitable or illegal material should be immediately reported to the police

10.4 Regular checks by Senior Staff will ensure that the filtering methods selected are appropriate, effective and reasonable.

10.5 Filtering methods will be selected by the school and will be age and curriculum appropriate.

11 AUTHORISING INTERNET ACCESS

11.1 All staff must read and sign the school's 'Staff Code of Conduct for ICT' before using any school ICT resources and any staff not directly employed by the school will be asked to sign the school's 'Acceptable Use of ICT Resources' document before being allowed internet access from the school site. Access to a school computer will only be allowed after the on screen 'Acceptable Use' agreement has been agreed to.

11.2 The school will maintain a record of pupils whose parents/carers have specifically requested that their child be denied internet or email access.

11.3 Parents/carers will be asked to sign and return the school's form stating that they have read and understood the school's 'Acceptable Use' document and give permission for their child to access ICT resources.

11.4 Staff will supervise access to the internet from the school site for all pupils, by line of sight supervision and remote monitoring though software.

12 PHOTOGRAPHIC, VIDEO AND AUDIO TECHNOLOGY

12.1 It is not appropriate to use photographic or video technology in changing rooms or toilets, apart from the use of CCTV when positioned appropriately and with proper safeguards in place for its use.

12.2 Staff may use photographic or video technology to capture to support school trips and appropriate curriculum activities.

12.3 Audio and video files may not be downloaded without the prior permission of the network manager.

13 ASSESSING RISKS

13.1 Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The senior leadership team should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

13.2 In common with other media such as magazines, books and video, some material available through the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

13.3 Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in school is allowed and methods to identify, assess and minimise risks will be reviewed regularly.

13.4 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

13.5 The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored.

13.6 Access to any websites involving gambling, games or financial scams is strictly forbidden and will be dealt with accordingly.

14 INTRODUCING THE POLICY TO PUPILS

14.1 Rules for internet access will be posted in all rooms where computers are used.

14.3 Pupils will be instructed in responsible and safe use before being allowed access to the internet and will be reminded of the rules and risks before any lesson using the internet.

14.4 Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.

15 CONSULTING STAFF

15.1 It is essential that teachers and learning support staff are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies:

- All staff are governed by the terms of the school's 'Staff Code of Conduct for ICT' and will be provided with a copy of the School Internet Policy and its importance explained.
- All new staff will be given a copy of the policy during their induction.

- Staff development in safe and responsible use of the internet will be provided as required.
- Staff will be aware that internet use will be monitored and traced to the original user. Discretion and professional conduct is essential.
- Senior managers will supervise members of staff who operate the monitoring procedures.

16 MAINTAINING ICT SECURITY

16.1 Personal data sent over the network will be encrypted or otherwise secured.

16.2 Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to emails.

16.3 The ICT Manager will ensure that the system has the capacity to deal with increased traffic caused by internet use.

17 DEALING WITH COMPLAINTS

17.1 Staff, children and young people, parents/carers must know how and where to report incidents. Concerns related to Safeguarding issues must dealt with through the school's Safeguarding Policy and Procedures.

17.2 The school's designated person for e-safety will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the headteacher immediately.

17.3 Pupils and parents/cares will be informed of the complaints procedure.

17.4 Parents/carers and pupils will work in partnership with the school staff to resolve any issues. 14.2 Responsible internet use, covering both school and home use, will be included in the PSHE curriculum.

17.5 As with drugs issues, there may be occasions when the school must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.

17.6 Sanctions for misuse may include any or all of the following:

- Interview/counselling by an appropriate member of staff
- Informing parents/carers
- Removal of internet access for a specified period of time, which may ultimately prevent access to files held on the system, including examination coursework.
- Referral to the police.

18 PARENTS/CARERS SUPPORT

18.1 Parents/carers will be informed of the school's E Safety Policy which may be accessed on the school website.

18.2 Any issues concerning the internet will be handled sensitively to inform parents/cares without undue alarm.

18.3 Advice on filtering systems and appropriate educational and leisure activities including responsible use of the internet will be made available to parents/carers.

18.4 Interested parents/carers will be referred to organisations such as Child Exploitation and Online Protection (CEOP).

18.5 A partnership approach will be encouraged with parents/carers and this may include practical sessions as well as suggestions for safe internet use at home.

19 COMMUNITY USE

19.1 School ICT resources may be increasingly used as part of the extended school agenda.

19.2 Adult users will sign the school's acceptable use policy.

19.3 Parents/carers of children and young people under 16 years of age will be required to sign the acceptable use policy on behalf of their child.

Arrangements for monitoring and evaluation

The Governing Body will evaluate the impact of this Policy by receiving data from the headteacher regarding the effectiveness of the procedures outlined above.