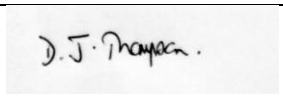
Keighley St Andrews C of E Primary School and Nursery

Online Safety Policy

Policy revised	**September 2017**
Date of Next Review	**September 2018**
Signed: Chair of Govs.	

The Online Safety Policy is part of the School Development Plan and relates to other policies including those for Computing, Anti-bullying and safeguarding. At Keighley St Andrews we ensure that our children are well educated around the dangers, as well as the advantages of Internet usage will minimize these risks.

Teaching and learning

Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning. Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

• Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
• Staff will guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
• Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
• Pupils will be shown how to publish and present information to a wider audience.

How does Internet use benefit education?
• educational and cultural exchanges between pupils world-wide;
• professional development for staff through access to national developments,
• educational materials and effective curriculum practice;
• access to learning wherever and whenever convenient;
• ICT provides access to experts in many fields for pupils and staff;
• access to world-wide educational resources including museums and art galleries.

Pupils will be taught how to evaluate Internet content
• The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
• Pupils will be taught the importance of cross-checking information before accepting its accuracy.
• Pupils will be taught explicitly about cyberbullying (For definition please see Appendix 1)
• Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or approaching a member of staff, who will report this using CPOMS following the online safety flowchart (Appendix 2).
• The evaluation of on-line materials is a part of every subject.

Managing Internet Access
Information system security
• School ICT systems security will be reviewed regularly.
• Virus protection will be updated regularly.
• Security strategies will be discussed with the Local Authority.
• The security of the school information systems will be reviewed regularly.
• Virus protection will be updated regularly.
• Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email.
• Files held on the school's network will be regularly checked.
• The Computing leader and ICT Technician will review system capacity regularly.

E-mail
• Pupils may only use approved e-mail accounts on the school system.
• Pupils must immediately tell a teacher if they receive offensive e-mail.

• In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
• Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
• The forwarding of chain letters is not permitted.
• Access in school to external personal e-mail accounts may be blocked.

Published content and the school website
• Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.
• The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
• The website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Publishing pupil's images and work
• Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Where possible, group photographs will be used rather than full-face photos of individual children.
• Pupils full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
• Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
• Work can only be published with the permission of the pupil and parents/carers.
• Pupil image file names will not refer to the pupil by name.
• Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Managing videoconferencing & webcam use
• Video conferencing should use the educational broadband network to ensure quality of service and security.
• Webcam use will be appropriately supervised for the pupils' age. Managing emerging technologies
• Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
• Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
• The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data
• Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Policy Implementation

Authorising Internet access

- All staff must read and sign the Acceptable Use Policy for ICT before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Handling Online Safety complaints

- Any Online Safety complaints or concerns (including accessing inappropriate content or instances of cyber bullying) must be reported using CPOMS.
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. (Child Protection flowchart of responses to an incident of concern.)
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Sanctions within the Behaviour Policy will include: interview/counselling by a Senior member of staff; informing parents or carers; removal of Internet or computer access for a period.
- The Computing leader will provide a termly report of all incidents to the head teacher, safeguarding lead and governing body.

Staff and the Online Safety policy

- All staff will be given the School Online Safety Policy and its importance explained.

• Staff will be informed that network and Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
• Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
• Staff will always use a child friendly safe search engine when accessing the web with pupils.
• Staff training in safe and responsible Internet use and on the school Online Safety Policy will be provided as required.

Enlisting parents' and carers' support
• Parents and carers attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and on the school website.
• A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
• Internet issues will be handled sensitively, and parents will be advised accordingly.
• The school will maintain a list of Online Safety resources for parents/carers.
• The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Approved by Governors: 20th September 2017

Appendix 1: Cyberbullying

Cyberbullying Overview

At Keighley St Andrews School, we offer a modern education supported by Christian values. A growing feature of our present age is the use of various communication devices. Mobile phones are ubiquitous and offer many facilities beyond simply the ability to make a phone call. The vast majority of phones provide free messaging, have cameras and video capacity and can connect to the internet allowing access to social networking websites.

Such technology and sites can be a powerful force for good. Mobile phones and social-networking sites can help to maintain friendships and provide links between people otherwise separated by geographical distance. The internet is a vital information tool for modern life. However, there are clearly risks over content and conduct with these media. Consequently, we value pupils knowing how to use these facilities appropriately and being able to identify and respond to inappropriate use, including cyberbullying.

Cyberbullying Definiton

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone".
This form of bullying is particularly insidious as it can invade home and school. Audiences can be large and reached rapidly. Words and images can easily become viral and difficult to control. The perpetrator may feel that they have anonymity and therefore feel more inclined to greater levels of bullying than might happen face to face. Images and words can be used separately or combined in an effort to belittle or ostracise others. Threats, harassment, embarrassment, humiliation, defamation or impersonation may all occur. Even where they are not the focus of an image, people may be displayed in the background of an image that is posted in a public e-space. Injury can therefore be occasioned by malice or by thoughtlessness and carelessness over the feelings of others. Such images and/or words are particularly damaging to the climate of trust within the school and may, in some circumstances, constitute illegal acts, necessitating reference to the police or other social agencies. Furthermore, offensive material may breach a provider's terms and conditions.

Cyberbullying - Who is Responsible?

This policy is intended to support online-safety for parents, staff and pupils alike and to identify responses to situations where cyberbullying has occurred. Incidents of cyberbullying occurring outside school may still be investigated and dealt with by the school. As with all aspects of health and safety, online-safety is the responsibility of everybody.

Cyberbullying - Prevention Preferable

Clearly, it is preferable to prevent all forms of bullying, rather than responding to it. At Keighley St Andrews School, we have a zero tolerance approach to all forms of bullying, including cyberbullying. Pupils are encouraged to discuss potential cases with staff, and all members of the school community receive training in a range of issues to do with bullying. This is extended to include parents and other stakeholders as appropriate. Furthermore, a range of software, including a firewall and anti-bullying software called SureProtect in combination with NetSupport DNA, allows our computing leader to limit ICT use, identify what internet sites have been used by members of the school network and helps to identify where inappropriate messages have been sent. Such monitoring is maintained at a level proportionate to need. Pupils are also educated in safe ICT use and sign in to computers through an Acceptable Use agreement every time they use a device.

Keighley St Andrews also has additional boundaries to ICT use that minimise the risk of cyberbullying occurring:

- pupils are not allowed to have mobile phones or other devices for social use within school.
- any recordings or images made by staff may only be made with express permission from a member of the Senior Leadership Team;
- pupils and staff may not share private telephone numbers or email addresses nor actively communicate with each other on social networking sites;
- laptops and other such devices may only be used with the school's express permission;
- social networking sites may not be accessed by pupils in school time or while on the school site;
- pupils may not access on-line email accounts - like, for example, Hotmail, Gmail or Yahoo - at school. Every pupil has their own personal school email account.

Cyberbullying - The Response

Nonetheless, if cyberbullying does occur, the issue is taken very seriously. All members of the Keighley St Andrews School community, staff, parents and pupils, are encouraged to report cyberbullying, whether they are directly involved or not, in the confidence that their concerns will be taken seriously. Any incidents of cyberbullying will be referred to a member of the Leadership Team through the online safety flowchart. If the incident includes a Child Protection issue, the Designated Safeguarding Lead will be informed. A log is kept of all bullying incidents. Information will only be shared with those who need to know in order to address the situation. As with other types of bullying, re-establishing the relationship between the person bullying and the person bullied will be facilitated by the school, unless the circumstances demand further action be taken.

Where an allegation of cyberbullying is made, the person making the complaint will be told not to respond but to retain all the evidence, such as texts, emails, screenshots and other communication. An investigation will be commenced on the same working day. As a condition of being a pupil at the school, the Designated Safeguarding Lead, or the safeguarding team, may require a pupil to give access to any data held on the internet, including the pupil's Facebook, or other social networking, accounts. Mobile phones, pc's and any other personal property may be searched to determine whether cyberbullying has occurred. Searching here includes, but is not limited to, a review of information held on internal and external electronic storage devices. Such measures will be used when there is a formal or informal cause for concern, including the circulation of rumours about pupil activities.

Where cyberbullying is found to have occurred, measures in the anti-bullying policy will be implemented.

Additionally, victims of cyberbullying will be encouraged to reconsider what information they keep and make publicly available on line, in order to prevent future occurrences. The offender will be required to stop immediately any inappropriate activities and remove unacceptable postings, whether textual, visual or auditory. Providers may be contacted to facilitate the removal of unacceptable material. Whether material is unacceptable will be decided by the school. Sanctions against the offending pupil, identified under the general anti-bullying policy, may be imposed subsequently.

Further measures in the case of cyberbullying may include:

- the pupil having access to ICT limited or withdrawn entirely in school;
- the incident being reported to the relevant service provider, potentially causing services and facilities to be withdrawn;
- notifying the police;
- where the school is unable to confirm the identity of a cyberbully or is caused to believe that there may have been an incident of 'identity theft', the police may be informed.
- In all cases, parents/carers of both the person bullying and the recipient will be informed.

Appendix 2: Inappropriate Activity Flowchart
If you are in any doubt, consult the Headteacher or DSL.