Lythe CEVC School
E-Safety Policy

E-safety co-ordinator: Lisa Armstrong
Designated Child Protection Co-ordinator: Sarah Alsop (Head Teacher)
E-safety / Child Protection Governor: Claudia Bloor

The policy is available for staff, parents & governors on the school website and by request from the school office.

This policy has been written in consultation with children (discussions in discrete e-safety lessons), parents (parent questionnaires), staff (staff meeting minutes) and governors (discussions in meeting – see minutes).

Policy approved by governing body: July 2015

Date for review: July 2016

Notes
NYCC Safeguarding procedures will be followed where an E-Safety issue occurs which gives rise to any concerns related to Child Protection.

NYSCB guidance documents are included as part of this e-safety policy:

Child Protection Procedures Section 9 – E-Safety: sexual abuse of children and grooming
http://www.safeguardingchildren.co.uk/section-9a-procedures.html

Safer working practice for Staff and volunteers working with Children and young people

www.safeguardingchildren.co.uk/safe-working-practices.html

Section A: Roles & Responsibilities

The Management Team accepts the following responsibilities:

- Identify a person (the E-Safety coordinator) (or team) to take responsibility for E-Safety and support them in their work.
- Ensure adequate technical support is in place to maintain a secure ICT system
- Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets
- Ensure liaison with the Governors
- Develop and promote an E-Safety culture within the school community
- Ensure that all staff and pupils agree to the Acceptable Use Policy and that new staff have E-Safety included as part of their induction procedures
- Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to E-Safety

- Receive and regularly review E-Safety incident logs; ensure that the correct procedures are followed should an E-Safety incident occur in school and review incidents to see if further action is required
- Take ultimate responsibility for the E-Safety of the school community

Responsibilities of the E-Safety Coordinator

- Promote an awareness and commitment to E-Safety throughout the school
- Be the first point of contact in school on all E-Safety matters
- Lead the school E-Safety team
- Create and maintain E-Safety policies and procedures
- Develop an understanding of current E-Safety issues, guidance and appropriate legislation
- Ensure delivery of an appropriate level of training in E-Safety issues
- Ensure that E-Safety education is embedded across the curriculum
- Ensure that E-Safety is promoted to parents and carers
- Ensure that any person who is not a member of school staff , who makes use of the school ICT equipment in any context, is made aware of the Acceptable Use Policy
- Liaise with the Local Authority, the Local Safeguarding Children's Board and other relevant agencies as appropriate
- Monitor and report on E-Safety issues to the E-Safety group, the Leadership team and Governors as appropriate
- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable
- Ensure an E-Safety incident log is kept up-to-date
- Ensure that Good Practice Guides for E-Safety are displayed in classrooms and around the school

Responsibilities of all Staff

- Read, understand and help promote the school's E-Safety policies and guidance
- Read, understand and adhere to the staff Acceptable Use Policy (AUP)
- Take responsibility for ensuring the safety of sensitive school data and information
- Develop and maintain an awareness of current E-Safety issues and legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times

- Embed E-Safety messages in learning activities where appropriate

- Supervise pupils carefully when engaged in learning activities involving technology

- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable

- Report all E-Safety incidents which occur in the appropriate log and/or to their line manager

- Ask NYCC technical staff to conduct occasional checks on files, folders, email and other digital content to ensure that the Acceptable Use Policy is being followed

- Ensure that suitable access arrangements are in place for and external users of the schools ICT equipment

- Respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home

- Liaise with the Local Authority and others on e-safety issues

Responsibilities of Pupils

- Read, understand and adhere to the pupil AUP and follow all safe practice guidance

- Take responsibility for their own and each others' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school

- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home

- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening

- Report all E-Safety incidents to appropriate members of staff

- Discuss E-Safety issues with family and friends in an open and honest way

Responsibilities of Parents and Carers

- Help and support the school in promoting E-Safety

- Read, understand and promote the pupil AUP with their children

- Discuss E-Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology

- Consult with the school if they have any concerns about their child's use of technology

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's E-Safety policies and guidance as part of the schools overarching safeguarding procedures

- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in E-Safety awareness

- Ensure appropriate funding and resources are available for the school to implement their E-Safety strategy

Responsibility of any external users of the school systems e.g. adult or community education groups; breakfast or afterschool club; visitors; students.

- Take responsibility for liaising with the school on appropriate use of the school's ICT equipment and internet

- Ensure that participants follow agreed Acceptable Use Procedures

Section B: Teaching & Learning

Electronic communication is part of the statutory curriculum and is a valuable teaching and learning tool for "doing better things and doing things better." Children use the internet and other means of electronic communication widely outside school and need to learn how to take control of their own safety and security.

Teachers will ensure that access to the internet is appropriate for the curriculum requirements and age and ability of pupils and should guide activities that will support appropriate learning outcomes. Children should always be supervised when using the internet.

E Safety is taught as a discrete unit of work in each year group in the school, and learning is applied in all subjects across the curriculum and encouraged out of school. By the end of KS2, children will have learned:

- how to use the internet for independent and appropriate research, and how to acknowledge sources of information and respect copyright.
- To interpret and critically evaluate information that they find online, with the knowledge that information may be untrue or biased, and to begin to distinguish between fact and opinion
- What to do if they find something inappropriate online in or out of school, including inappropriate contact from adults
- How to protect themselves from the inappropriate use of technology by others and the need to respect the rights of other users
- How to deal with unsolicited information (pop-up advertising, spam etc.)
- What personal information is, including passwords and personal thoughts and opinions, and why it is important to protect this
- To use a range of forms of online communication appropriately for formulating, developing and exchanging ideas, and to be aware their benefits and associated risks
- To identify the characteristics of people online who are worthy of their trust
- The importance of understanding and following the school's Acceptable Use Policy
- About the issues surrounding cyber-bullying and to understand the impact on an individual of sending or uploading unkind or inappropriate content
- What steps to take in the event of experiencing cyber-bullying

Creating online content (as part of the curriculum):

As part of the curriculum we encourage pupils to create online content. Pupils are taught safe and responsible behaviour in their creation and publishing of online content. They are taught to publish for a wide range of audiences which might include governors, parents or other children. Blogging, podcasting and other publishing of online content by pupils will take place using the school website or other media selected by the school. Pupils will only be allowed to post or create content on sites where members of the public have access when this is part of a school related activity. Appropriate procedures to protect the identity of pupils will be followed.

We take all steps to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright.

Section C: Use of Electronic Communications

E-mail

Whole -class email addresses must be used for pupil communication outside of the school and emails should not be sent or received without a teacher's permission. Care should be taken when opening attachments, and attachments in unsolicited e-mails should not be opened.

Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

Website

The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Images, videos, or sound recordings that include pupils will be selected carefully. Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents or carers will be obtained before images/videos/sound recordings of pupils are electronically published and staff should be made aware of which children are not to be photographed. Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

Social Networking & Personal Publishing

At the time of writing, no form of social networking is permitted in school other than education-specific social networking resources (eg Makewaves, Maths Nrich). Children should not be asked to use any other social networking sites, blogs, wikis, mobile devices etc. at home. Use of approved sites should be carefully monitored by the teacher.

At the time of writing, families are permitted to take photographs and videos of their **own children only** at school events. If photographs or videos contain images of **other families' children,** these pictures **must not under any circumstances** be published in any way online. If this is found to happen, photographing of school events will be banned in future.

Using video conferencing and other online meetings

Video conferencing may be used to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. We will ensure that staff and pupils take part in these opportunities in a safe and responsible manner. All video conferencing activity is to be supervised by a suitable member of staff. Pupils will not operate video conferencing equipment, answer calls or set up meetings without permission from the supervising member of staff.

Video conferencing equipment is to be switched off and secured when not in use and online meeting rooms will be closed and logged off when not in use. All participants will be made aware if a video conference is to be recorded. Permission is sought if the material is to be published.

A video conference or other online meeting between a member of staff and pupil(s) which takes place outside school or whilst the member of staff is alone is not allowed.

Mobile phones and personal devices.

All mobile phones and personal electronic devices are banned in school for pupils. The school accepts no responsibility for the loss, theft or damage of such items.

School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour, bullying or children protection policy. The phone or device may be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile device may provide evidence relating to a criminal offence, the phone will be handed over to the police for further investigation.

If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers or to children with parents/carers' permission.

If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone.

Pupils will be instructed in safe and appropriate use of mobile phones and personal device in e-safety lessons and will be made aware of boundaries and consequences.

If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Head Teacher.

Section D: Administration and Management

Information Systems

Maintenance of technical aspects of the ICT system in relation to the security of the school information systems is the responsibility of North Yorkshire Schools ICT and they are responsible for virus protection.

Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

School recognises their obligation to safeguard staff and pupil's personal data including that which is stored and transmitted electronically. Any personal or sensitive data taken off-site will be encrypted (teaching staff **and governors** have all been provided with encrypted memory sticks). **As per the Acceptable Use Policy, information must be deleted from memory sticks as soon as possible.**

- All computers or laptops holding sensitive information are set up with strong passwords, password protected screen savers and screens are locked when they are left unattended
- Staff are provided with appropriate levels of access to the schools management information systems holding pupil data. Passwords are not shared and administrator passwords are kept securely
- Only the headteacher and school administrator are permitted to use the administration computers in the school offices
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside school
- When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
- We follow NYCC procedures for transmitting data securely and sensitive data is not sent via e-mail unless encrypted.
- Remote access to computers is by authorised personnel only
- We have full back up and recovery procedures in place for school data
- Where sensitive staff or pupil data is shared with other people who have a right to see the information, for example Governors or the SIP, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies.

Pupils are taught about the need to protect their own personal data as part of their E-Safety awareness and the risks resulting from giving this away to third parties

Unapproved software should not be downloaded and portable media should not be used without scanning for viruses and malware.

Filtering

The school's broadband access will include filtering appropriate to the age and maturity of pupils and is the responsibility of NYCC Schools ICT. However, there is no guarantee that inappropriate sites will not be accessible and teachers are responsible for checking the content of websites before use with children and particularly checking the results of image searches. Any unsuitable sites should be reported to the ICT Co-ordinator at once, who will then record the incident and escalate the concern as appropriate (see sheet "Response to an Incident of Concern").

The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.

Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, NYCC Police or CEOP.

School Network

The server is password protected with the password known to the school's ICT technicians, Head Teacher, Office Administrator and ICT co-ordinator. The wireless network is protected by a secure log on to prevent unauthorized access.

Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Pupils will be instructed about safe and appropriate use of personal devices both in school and at home in accordance with the school Acceptable Use Policy.

Authorisation of internet access

All pupils are authorised to use computers and the internet under staff supervision. At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials. At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

All users of the internet will read and sign the Acceptable Use Policy before using any school ICT resources.

Parents will be asked to read and sign the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate (see below).

When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

Risk Assessment

The school will take all reasonable precautions (including checking search terms, especially for image searches, before asking children to use them) to ensure that children access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor NYCC can accept liability for the material accessed, or any consequences resulting from Internet use.

The school will use the 360º Safe Self-Review Tool to establish that the e–Safety policy and procedures are adequate.

Methods to identify, assess and minimise risks will be reviewed regularly. The E-Safety Co-ordinator will collect the views of members of the E-Safety Team when doing this.

Section E: Response to Incidents of Concern

All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).See separate "Response to Incident of Concern" sheet which is displayed in the staff room. Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's SafeguardingTeam or e-Safety officer and escalate the concern..

The E-Safety Coordinator will record all reported incidents in school and actions taken in the School E-Safety incident log (in Chronologies in staff area of computer) and other in any relevant areas e.g. Bullying or Child protection log.

The Designated Child Protection Coordinator will be informed of any E-Safety incidents in or out of school involving Child Protection concerns, which will then be escalated appropriately.

The school will manage E-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.

The school will inform parents/carers of any incidents of concerns as and when required.

After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer. If an incident of concern needs to be passed beyond the school then the concern will be escalated to the County e-Safety officer to communicate to other schools in North Yorkshire.

Handling e-safety complaints

Complaints about Internet misuse will be dealt with under the School's complaints procedure, which will be shared with staff and parents. Incidents arising out of school will not be investigated under the school's procedures.

Any complaint about staff misuse will be referred to the head teacher.

All E–Safety complaints and incidents will be recorded by the school, including any actions taken.

Parents and pupils will need to work in partnership with the school to resolve issues.

All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.

All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour, and these policies will be followed when dealing with cases of cyberbullying.

All incidents of cyberbullying in school will be recorded.

Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence, to not respond to bullying messages, and to report incidents as soon as possible.

The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary. A service provider may be contacted to remove content if the bully refuses or is unable to delete content.

Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

In addition to sanctions in the bullying policy, sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance with our anti-bullying policy, behaviour policy or Acceptable Use Policy.
- The Police will be contacted if a criminal offence is suspected.

Discussion of the e-safety policy

The E–Safety Policy will be formally provided to and discussed with all members of staff, pupils, parents and governors. Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

Section F: Parental Involvement

Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website. Parents will be requested to sign the children's AUP and discuss its implications with their children.

A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days.

Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents. Interested parents will be referred to useful organizations.