SCALBY LEARNING TRUST

E-Safety Policy

HISTORY OF DOCUMENT

Issue No.	Author	Date Written	Approved by Governors	Comments
1	NYCC	23.03.14		
2	Emma Choat	5.1.15	21.1.15	New Policy adopted
3			24.5.17	Minor name changes

Member of staff responsible: Assistant Headteacher, Behaviour & Safety

Introduction

This policy was informed by:

- DfE guidance on e-Safety in schools, 2012
- UK Council for Child Internet Safety (UKCCIS) guidance 2012
- CEOP guidance for schools and educational settings 2013
- Programme of Study for PSHE, National Curriculum 2007
- Programme of Study for Information Technology, National Curriculum 2007

1. Statutory Obligations

Every school has a statutory responsibility to have:

- An up to date e-safety policy.
- To deliver e-safety education through the relevant programmes of study within the national curriculum and pastoral initiatives.
- To prepare all students for the responsibilities of adult life.

Scalby School recognises that it also has its part to play in promoting national and local initiatives to help safeguard young people in relation to internet use and emerging technologies. These include:

- having an up-to-date e-safety policy consistent with DfES 2012 guidelines
- having an effective implementation process for the e-safety policy with subsequent monitoring and evaluation strategies
- having an effective and developmental e-safety programme in each key stage
- for all young people identified as being vulnerable to receive the appropriate education, advice, information and support about e-safety both in and out of school.

In addition we see e-safety as a core component of effective curriculum provision.

The Headteacher and Governing body have a legal responsibility to safeguard children and staff and this includes online activity.

- The school has appointed an e–Safety Coordinator
- The School has appointed the Child Protection governor –to take lead responsibility for e-Safety

Teaching and learning

Internet use is part of the statutory curriculum and is a necessary tool for learning, the Internet is a part of everyday life for education, business and social interaction. The Federation has a duty to provide students 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 access is an entitlement for all students.

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between students worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for students and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with NYCC and DfE;
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and students complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of students.
- Staff should guide students to online activities that will support the learning outcomes planned for the students' age and ability.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will students learn how to evaluate Internet content?

Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Students will use age-appropriate tools to research Internet content.

The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Managing Information Systems

How will information systems security be maintained?

- The Server must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date by IT Support.
- Virus protection for the whole network has been installed and will be kept current by IT Support.
- Access by wireless devices will be proactively managed and secured with a minimum of WPA2 encryption.

The Schools Broadband network is protected by a cluster of high performance firewalls.

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet will be encrypted or coded to hide the identity of the individuals.
- All downloaded software must be approved by the IT Support Manager
- The use of user logins and passwords to access the school network will be enforced.

How will email be managed?

IT support currently filter some spam and unrecognised email.

- Students may only use approved email accounts for school purposes.
- Students must immediately tell staff if they receive offensive email.
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole -class or group email addresses will be used for communication outside of the school.
- Staff will only use official school provided email accounts to communicate with students and parents/carers, as approved by the IT Support Manager

How will published content be managed?

The contact details on the website should be the school address, email and telephone number. Staff or students' personal information must not be published.

The Headteacher 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.

Can students' images or work be published?

- Images or videos that include students will be selected carefully and will not provide material that could be reused.
- Students' 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 of students are electronically published.
- Written consent will be kept by the school where students' images are used for publicity purposes, until the image is no longer in use.
- The School will have a policy regarding the use of photographic images of children which outlines policies and procedures.

How will filtering be managed?

- The school's broadband access will include filtering appropriate to the age and maturity of students.
- The school will work with NYCC IT Support to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all students) will inform the IT Manager.
- If staff or students discover unsuitable sites, the URL will be reported to the IT Manager who will then record the incident and escalate the concern as appropriate.
- Any material that the school believes is illegal will be reported to NYCC IT Support.

How will videoconferencing be managed?

- Videoconferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education.
- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- The equipment must be secure and if necessary locked away when not in use.

Users

- Students will ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the students' age and ability.
- Parents and carers consent should be obtained prior to children taking part in videoconferences.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

How are emerging/new technologies managed?

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

Students will be instructed about safe and appropriate use of personal devices

How should personal data be protected?

The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

Schools will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.

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

How will Internet access be authorised?

- All staff will read and sign the 'Acceptable Use Agreement' Policy before using any school ICT resources.
- All visitors to the school site who require access to the schools network or internet access will be reminded of the Acceptable Use Policy.
- Parents will be informed that students will be provided with supervised Internet access appropriate to their age and ability.
- 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).

Curriculum access

- As appropriate to Key Stage 3 and 4 progression, students will be generally supervised. Students will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.
- Students will agree to comply with the School e–Safety Rules as displayed in the classrooms.

How will risks be assessed?

The school will take all reasonable precautions to ensure that users 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. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

The IT Support Manager will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches may be reported to North Yorkshire Police.

Methods to identify, assess and minimise risks will be reviewed regularly.

How will the school respond to any incidents of concern?

- All members of the school community will report e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc) to the ICT Coordinator.
- The IT Support Manager will record all reported incidents and actions 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 involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school 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.
- 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 Safeguard Team or e-Safety officer and escalate the concern to the Police.
- 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 and/or the County e-Safety Officer.

How will e–Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the school's complaints procedure.
- Any complaint about staff misuse will be referred to the Headteacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Students and parents will be informed of the complaints procedure.
- Parents and students 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.

How will Cyberbullying be managed?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects.

It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the

Education and Inspections Act 2006:

- **every school must have measures to encourage good behaviour and prevent all forms of bullying amongst students. These measures should be part of the school's behaviour policy which must be communicated to all students, school staff and parents**
- **gives headteachers the ability to ensure that students behave when they are not on school premises or under the lawful control of school staff.**

Where bullying outside school (such as online or via text) is reported to the school, it should be investigated and acted on.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed they should seek assistance from the police.

For more information please read "Preventing and Tackling Bullying: Advice for School

Leaders, Staff and Governing Bodies"

http://www.education.gov.uk/aboutdfe/advice/f0076899/preventing-and-tackling-bullying

DfE and CEOP have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.ceop.police.uk/safety-centre/

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.

There are clear procedures in place to support anyone in the school community affected by cyberbullying-contact the Headteacher.

All incidents of cyberbullying reported to the school will be recorded.

Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.

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.

Students, 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.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for students and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of students will be informed.
- The Police will be contacted if a criminal offence is suspected.

Informing students of the contents of this policy:

Teaching e-safety.- This could be as an ICT lesson activity, part of the pastoral programme or part of every subject whenever students are using the internet.

Useful e–Safety programmes could include:

- **Think U Know:** www.thinkuknow.co.uk
- **Childnet:** www.childnet.com
- **Kidsmart:** www.kidsmart.org.uk
- **Orange Education:** www.orange.co.uk/education
- **Safe:** www.safesocialnetworking.org

All users will be informed that network and Internet use will be monitored.

- An e–Safety training programme will be established across the Federation to raise the awareness and importance of safe and responsible internet use amongst students.
- Pupil instruction regarding responsible and safe use will precede Internet access.
  - An e–Safety module will be included in the Life and ICT programmes covering both safe school and home use.
  - e-Safety rules will be posted in all rooms with Internet access.
  - Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
  - Particular attention to e-Safety education will be given where students are considered to be vulnerable.

Informing staff of the contents of this policy:

The e–Safety Policy will be formally provided to and discussed with all members of staff.

- To protect all staff and students, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- 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.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Informing Parents of the contents of this policy:

Internet use in students' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, students may have unrestricted and unsupervised access to the Internet in the home. The school may be able to help parents plan appropriate, supervised use of the Internet at home and educate them about the risks.

Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.

- A partnership approach to e-Safety at home and at school with parents will be encouraged.
- Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.
- Parents will be encouraged to read the school rules for using the internet and discuss implications with their children.
- 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 on request.
- Interested parents will be referred to organisations listed in the "e–Safety Contacts and References section".

Schools e-Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Staff that could contribute to the audit include: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Network Manager and Head Teacher.

Has the school an e-Safety Policy that complies with guidance?	Y/N
Date of latest update:	
Date of future review:	
The school e-safety policy was agreed by governors on:	
The policy is available for staff to access at:	
The policy is available for parents/carers to access at:	
The responsible member of the Senior Leadership Team is:	
The governor responsible for e-Safety is:	

The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Were all stakeholders (e.g. students, staff and parents/carers) consulted with when updating the school e-Safety Policy?	Y/N
Has up-to-date e-safety training been provided for all members of staff? (not just teaching staff)	Y/N
Do all members of staff sign an Acceptable Use Policy on appointment?	
Are all staff made aware of the schools expectation around safe and professional online behaviour?	Y/N
Is there a clear procedure for staff, students and parents/carer to follow when responding to or reporting an e-Safety incident of concern?	Y/N
Have e-safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	Y/N
Is e-Safety training provided for all students (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y/N
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all students?	Y/N
Do parents/carers or students sign an Acceptable Use Policy?	Y/N
Are staff, students, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit been initiated by SLT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements?	Y/N
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	Y/N
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?	Y/N
Does the school log and record all e-Safety incidents, including any action taken?	Y/N
Are the Governing Body and SLT monitoring and evaluating the school e-Safety policy and ethos on a regular basis?	

e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Children's Officer for Training & Development, Children's Safeguards Team, Families and Social Care, Kent County Council. The Children's Officer for Training & Development is Mike O'Connell email: mike.oconnell@kent.gov.uk Tel: 01622 696677

Children's Safeguards Team: www.kenttrustweb.org.uk?safeguards

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

EiS - ICT Support for Schools and ICT Security Advice: www.eiskent.co.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

*This Policy was reviewed by the Governors on a **2** yearly cycle and must be signed by the Chair of Governors and Headteacher.*

Policy Reviewed: May 2017	
Next Review: May 2019	
Signature of Chair of Governors:	Signature of Head Teacher:

Please ensure you complete the Equality Impact Assessment below

Equality Impact Assessment Form

1. Title of policy, project or practice being reviewed or planned

E safety policy

2. Outline the aims, objective and purpose of the change including any positive impacts on equalities groups.

N/A

3. Which groups of people (if any) are most likely to be affected by the planned changes, positively or negatively?

N/A

4. Does, or could these changes have an adverse effect on members of an equalities group? Identifying a negative impact is not a problem, as it gives you an opportunity to remove the barrier, find a way around it, or offer an alternative.

Protected Characteristics / Group	Yes (brief explanation)	No
Age (staff only)		x
Disability		x
Gender		x
Gender reassignment		x
Marriage / civil partnership		x
Pregnancy / maternity		x
Race / ethnicity		x
Religion / belief		x
Sexual orientation		x

5 Is there a way to modify the decision to remove or mitigate the negative impact on protected groups while still achieving this aim? How can you maximise positive outcomes and foster good relationships?

n/a

As E-safety is regularly discussed as part of the standing safeguarding item at SLT weekly meetings, this helps to regularly monitor whether the policy is fit for purpose.

6 Outline the decision made and actions planned.

n/a