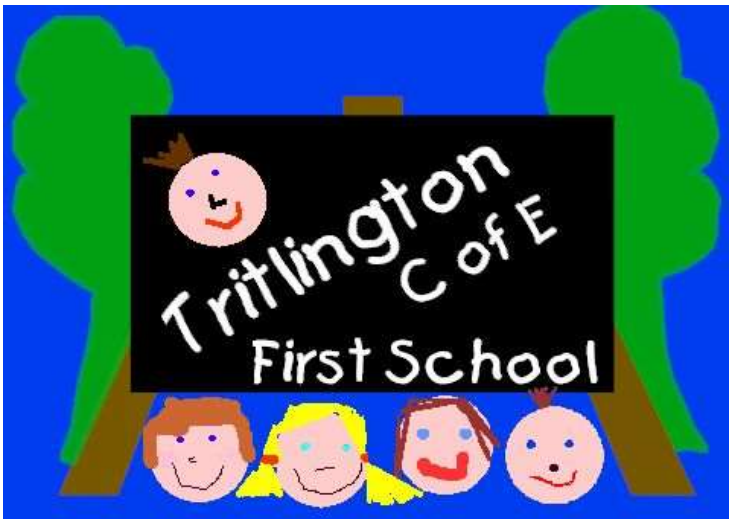
E-safety Policy



Northumberland

County Council

Presented to Governors Jan 2017. Ratified Spring Term 2017

Tritlington C of E Aided First School

Ethos

Reflecting the Trust Deed, the school will preserve and develop its religious character in accordance with the principles of the Church of England and in partnership with the Church at parish and diocesan level.
The school will aim to serve its community by providing an education of the highest quality within the context of Christian belief and practice. It encourages an understanding of the meaning and significance of faith and promotes Christian values through the experience it offers all pupils.
These values include love, caring, sharing, forgiveness, tolerance, perseverance and goodwill to all people.
We aim to ensure everyone reaches their full potential by providing an education that stretches the mind the mind, strengthens the body, enriches the imagination, nourishes the spirit, encourages the will to do good and opens the heart to others

Our Mission Statement

As a Church of England school, we promote the Christian values of love, friendship, forgiveness, tolerance, perseverance and goodwill to all. Members of the school community are encouraged to thrive and achieve as individuals; where every person really does matter; in a setting that respects and celebrates differences.

Our Vision Statement

The school will develop its Christian character in accordance with the Church of England. We aim to ensure that everyone reaches their full potential by providing an educational environment that stretches the mind, strengthens the body, enriches the imagination, nourishes the spirit and encourages the will to do good and open the heart to others.

Headteacher: Mrs H Hughes
E-Safety Co-ordinator: Mrs K Stephenson
The Designated Child Protection Co-ordinator: Mrs H Hughes
E-safety Governors: Mrs L Crofts and Mrs A Slavin
Technician: Mr M Nieurzyla
ICT Subject leader: Mrs K Stephenson

Tritlington C of E Aided First School

E Safety Policy

Rationale

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing.

The school's e-safety policy will operate in conjunction with other Policies:

- Behaviour
- Anti bullying
- Child Protection
- Curriculum
- Data Protection
- Use of images

E-Safety relies on effective practice at a number of levels:

- Responsible ICT use by all staff and students encouraged by education and made explicit through published policies
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering
- The appointment of an e-safety Coordinator to implement and manage this policy
- The support of the Headteacher and Governing Body

Principles

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community. The monitoring and implementation of the e-safety policy is delegated to the E Safety co-ordinator/ ICT subject leader.

- The E-Safety Officer will attend county CPD training at least every three years to enable carrying out of e-safety roles and training of other colleagues, as relevant.
- E-safety measures will be reviewed every two years or more regularly in the light of any significant new developments in the use of the technologies, new purchase of hard or software, new threats to e-safety or incidents that have taken place.

- Effective filters will be in place and access to unsuitable materials which the filter has not identified will be reported to County Hall E-safety staff.
- The Headteacher and e-safety officer will monitor policy central reports and investigate any new word or high frequency areas.
- The school will deal with any incidents perpetrated by pupils in line with bullying and behaviour policies, and perpetrated by staff in line with disciplinary procedures.
- Where an incident is in the area of child protection the school's flow chart of actions will be followed.
- E – safety information will be available to parents.

Introduction

At Tritlington we value the use of new technologies for both teaching and learning. We recognise that electronic communication, website use and mobile technologies have become integral to the lives of our pupils, both within schools and in their lives outside school. New technologies will continue to be relevant to our pupils in their futures, for continuing education, employment and recreation.

Children at Tritlington have an entitlement to safe internet access, which is part of the school's wider duty of care. With the support of Northumberland County Council, we take steps to limit the risks associated with internet use, whilst recognising that it is impossible to eliminate all risks. We acknowledge that many of the risks associated with internet use mirror those which exist in the offline world. For this reason we educate children to be aware of the dangers of internet use, to know how to avoid them and when to ask for help.

We recognise that as a school we have a responsibility in educating parents about the dangers as well as the benefits of internet use. Parents are encouraged to supervise internet use and be aware of their children's online behaviour in order to promote safe use.

The school's e-safety procedures ensure safe and appropriate use of the internet by staff and pupils and should be read in conjunction with other policies including behaviour, child protection and anti-bullying policies.

The purpose of this policy is to:

- Establish the ground rules that are in place at Tritlington C of E Aided First School for using the internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate the pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
- Describe how these fit into the wider context of our discipline and PSHE policies.
- Demonstrate the methods used to protect children from accessing sites containing inappropriate material such as pornography, racist or politically extreme views and violence.

The Policy

The structure of the ICT provision at Tritlington and the safety features put in place as part of the Northumberland ICT SLA encompass the following:

- Prevention or limitation of access to illegal, harmful or inappropriate images or other content
- Blocked access to inappropriate websites
- Teacher vigilance to ensure that inappropriate activities are not carried out using computers in free time
- No use of computers without direct supervision by teaching staff
- The use of an individual username and password for all children, although for some sites children up to Year Two may use a shared password for some educational activities and shared documents
- Weekly policy central reports on usage and violations from SLA to Senior Leadership and ICT staff

E-safety teaching at Tritlington includes the following at age appropriate levels:

- Awareness about the need to avoid sharing of personal information including sending compromising images
- Awareness of being subject to grooming by those with whom they make contact on the internet
- Encouragement to make online friends only with people they know in the offline world
- Knowledge of how to deal with Cyber-bullying
- Understanding that they could be involved in Cyber-bullying as a victim or perpetrator
- Understanding that downloading could involve illegal activity or be damaging to the hardware, and encouraging children to ask for help
- Awareness that excessive computer use could lead to physical, social or emotional damage to the child

The Procedure

Children are taught to treat the hardware with respect and to follow behaviour routines and safe usage procedures.

- When children log on to the network they have to agree to a safe usage policy on every occasion. This is explained and discussed at the start of every year and repeated when an incident or misunderstanding has occurred.
- The school ensures that users may only access the school's networks through a password and personal log-in. Children are given a password which is available to the teacher, and teachers can use their own log-in to access all pupil files.
- Staff are able to change their own passwords. Children are taught the importance of password security.
- Parents are asked to sign an acceptable use policy and to share the requirements with their children.
- Safer Internet Day (SID) is observed annually in school. There are assemblies suitable for both key stages and suggested materials for use in class. Older

children make posters about safe internet use and cyber-bullying (including mobile phone usage) which are displayed around school.

- Tips for safe internet use at home are shared with parents at least once each year, to coincide with SID and in response to any reported issues with internet usage in school or at home. These are shared through the school newsletter and separate booklets. We provide a range of information to support parents with E-safety on the school website.

Teaching and Learning

- The internet is an essential element in 21st century life for business and social interaction. The school has a duty to provide children and staff with quality internet access as part of the learning experience.
- Internet access is part of the statutory curriculum and a necessary tool for students and staff
- The school's curriculum internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils through the installation of Policy Central Enterprise (PCE) provided by the Local Authority
- Pupils are taught about acceptable internet use and are given clear objectives for internet use
- Pupils and staff are expected to acknowledge and agree to the acceptable use policy when logging onto the curriculum system with their individual passwords
- Pupils are taught about effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school ensures that the use of the internet derived materials by staff and pupils complies with copyright law
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Using Technologies

Internet Access

- The school's curriculum ICT system is monitored by PCE which sends weekly updates to the E-Safety co-ordinator regarding unacceptable use of the system. This identifies individual pupils, staff or computers which have been used and reports on the types of inappropriate access. This can then be managed according to the school's behaviour policy.
- Virus protection is updated regularly
- Staff are not permitted to access the school's wireless technology with their personal laptops unless PCE is installed.
- Staff using school laptops at home are aware that PCE is installed on all units and that the appropriate use of the equipment will be monitored when the laptop accesses the school's wireless system on its return to school.

E-Mail

- Pupils may only use approved e-mail accounts on the school system where available

- Pupils must immediately tell a teacher if they receive offensive material or comments via e-mail
- Pupils must not reveal personal details of themselves or others in electronic communication, or arrange to meet anyone
- E-Mail sent to an external organisation must be authorised before sending, in the same way as a letter written on school headed paper.
- Staff should not give out personal e-mail addresses to children or parents without discussing the implications of this with the e-safety coordinator and Headteacher.

School Website

- Tritlington's contact details are on the school website. The school address, e-mail and telephone number are all available here.
- Staff and pupil details or personal information is not published.
- The Headteacher has overall editorial responsibility and ensures that the content of the school website is accurate and appropriate.
- Photographs that include pupils are selected carefully so that they do not enable individual children to be clearly identified
- Pupil's full names are not used anywhere on the website
- Written permission from parents/carers is obtained before photographs of pupils are published on the website

Social networking and personal publishing

- The school blocks access to social networking sites
- Newsgroups are also blocked
- Pupils are taught never to give information which may allow them to be identified
- Staff are provided with guidance to support their safe use of social networking sites out of school.

Mobile Phones

- In order to ensure the safety of both children and staff, mobile phones are not allowed in the vicinity of children during the school day.
- Staff mobile phones should be turned off /left on silent in the staff room or school office at all times during teaching sessions. If it is felt necessary to make phone calls/take messages during the school day this must occur during lunch / break times in an area where there are no children (e.g. the staff room).
- Staff should use the school mobile phone when off site
- Staff should not give out personal mobile numbers to pupils or parents
- Pupils are not permitted to bring mobile phones and other devices with photographic / video capability (eg ipods) into school except with the express permission of the Headteacher / senior staff.

Photographs

At Tritlington we value the use of photographs in our school displays; on our walls, in children's workbooks, and on our website**.**

- Parents are asked annually if they wish to give their permission for photographs to be used in school, on the website or in advertising/publicity materials. (Parents can agree to some, all or none of the above as they see fit).
- We undertake not to take indecent photographs and not to identify individuals in the photographs that are used online or in any publicly distributed materials.
- Staff may only use school's equipment to take pupil photographs during lessons and other activities including school outings. These photographs must only be uploaded to the school's network.
- Children are encouraged to take photographs themselves, and to be aware of taking a decent image which others are happy with.
- Parents and volunteers who accompany outings or attend school events such as assemblies, plays or sports days are asked not to take or distribute photographs without permission of the parents of the children in them. Parents are also reminded on every such occasion that they must not share photographs or videos on social network sites.
- Photographs/videos taken during school trips should only be taken by staff members on school cameras which are directly downloaded into the appropriate folder on the school network.
- If pupils use the school cameras, the teacher responsible for the group should supervise the shot where possible.
- Parent volunteers on trips are instructed that they are not allowed to take photographs on their mobile phones
- All photographs taken by children and staff should be scrutinised by the teacher for suitability before being used for any purpose

Managing Technologies

Emerging technologies are evolving at a rapid rate and although every attempt is made to protect children from offensive or inappropriate material and misuse, there may be occasions when inadvertent access occurs. The following points apply:

- If staff or pupils discover an unsuitable site, it must be reported immediately to the teacher and then the E-Safety Co-ordinator, who will report the site to the appropriate person in the Local Authority (Richard Taylor / John Devlin) to ensure that the site is blocked.
- If it is felt that the incident is a child protection issue, the flow chart for reporting this will immediately be put into place.
- All internet access including e-mails will be monitored through PCE on the curriculum network. The admin system is protected by a separate firewall system.
- All photographs / videos should be viewed by the teacher for appropriateness before publishing openly. Photographs which may cause the subject to be embarrassed or upset should be deleted.
- Any child taking photographs deemed to be inappropriate should be dealt with in terms of the behaviour policy.

Policy Decisions

- All staff and pupils must agree to the ICT acceptable use policy, (AUP).
- The AUP is regularly explained to the children at their level to ensure their understanding.
- The AUP is included in the home / school agreement to ensure that parents are aware of the high priority that the school places on the safe use of technologies.
- PCE reports are regularly monitored by the E-Safety co-ordinator who in turn reports to the Headteacher and governors.
- The school keeps a record of all staff and pupils who are granted internet access.
- At Key Stage 1 / Early Years, access to the internet will be by adult demonstration with directly supervised access to approved online materials
- At Key Stage 2, access to the internet will be by supervised access to online materials filtered by PCE

Assessing Risks

- The school takes all reasonable precautions to ensure that users access only appropriate material through the use of PCE systems. Supervised access is always recommended as the school is aware that no firewall system is completely infallible.
- The school audits ICT provision on an annual basis to establish if the E-safety Policy is adequate and that its implementation is effective.

Handling E-Safety complaints

- The E-Safety co-ordinator is responsible for regularly monitoring internet use and updates the Headteacher and Governors on a termly basis
- The E-Safety Co-ordinator will inform class teachers if it is felt that there has been an infringement of the AUP by a child in the class. Minor infringements will first result in a warning given to the child. Further or more serious infringements will be dealt with under the school's behaviour policy
- Any infringement of the school policy by pupils or staff which is deemed to be a child protection issue will immediately be reported to the appropriate authorities via the flow chart system (see appendix 4).
- Incidents where staff or pupils are suspected of having obscene images on a mobile device will be dealt with via the flow chart system.

Policy reviewed: March 2016

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved online materials.	Web directories e.g. Ikeep bookmarks Webquest UK NGFL Learning Zone The school / cluster VLE
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick
Exchanging information with other pupils and asking questions of experts via email or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.	RM EasyMail SuperClubs Plus School Net Global Kids Safe Mail NGFL Learning Zone Cluster Microsite Blogs
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted. Pupils' work should only be published on "moderated sites" and by the school administrator.	Making the News SuperClubs Plus Headline History NGFL Learning Zone Cluster Microsites National Education Network Gallery
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought.	Making the News SuperClubs Plus Learninggrids

	Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws	Museum sites, etc. Digital Storytelling BBC – Primary Art Cluster Microsites National Education Network Gallery
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Plus FlashMeeting

Appendix 2: Useful resources for teachers

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/
Becta
http://schools.becta.org.uk/index.php?section=is
Chat Danger
www.chatdanger.com/
Child Exploitation and Online Protection Centre
www.ceop.gov.uk/
Childnet
www.childnet-int.org/
Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
Digizen
www.digizen.org/
Kidsmart
www.kidsmart.org.uk/
Think U Know
www.thinkuknow.co.uk/
Safer Children in the Digital World www.dfes.gov.uk/byronreview/

Appendix 3: Useful resources for parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
Childnet International "Know It All" CD
http://publications.teachernet.gov.uk
Family Online Safe Institute
www.fosi.org
Internet Watch Foundation
www.iwf.org.uk

Parents Centre
www.parentscentre.gov.uk
Internet Safety Zone
www.internetsafetyzone.com

Appendix 4: Response to an E Safety incident

REPORTING AN E-SAFETY INCIDENT - ALL SETTINGS

SETTING

IMMEDIATE ACTION

A CONCERN IS RAISED
Seek advice from the designated person for e-safety and/or Local Authority

Secure and preserve all evidence and hardware in the interim

This might mean isolating a machine and making sure it's not used, do not switch off the device as this might lose important evidence

Inform your senior manager and child protection staff

Make a written record of the concern and your actions

LOCAL AUTHORITY

NCC & School networks
Contact JD/RT to discuss incident and plan of action
john.devlin@northumberland.gov.uk /
richard.taylor@northumberland.gov.uk

JD/RT to coordinate the investigation of the incident

Liaise with the e-safety lead in setting, Info Services security team, legal service and police as appropriate

Are there any Child Protection concerns?

No

Yes Contact LADO

LADO will agree a strategy for intervention
Within 1 working day

Possible referral to:
- Northumbria Police Specialist Investigation Unit
- CS e-safety SLA Team
- FACT Locality Office

JD/RT organise internal investigation, liaise with setting and report
this might include: PCE analysis, forensic examination and securing of equipment, liaison with Info Services security team, liaise with legal service and police

Non-NCC Networks

Follow your relevant e-safety Incident Reporting and Child Protection procedures and agree a strategy for dealing with the incident.

For information and advice, contact the Local Authority Designated Officer (LADO)

Chris.O'Reilly@northumberland.gcsx.gov.uk

ALL PARTIES

Report to Designated Officer for e-safety, School, Head of Service

REVIEW by LA and School:
Consider whether the incident has procedural, training or security implications. Share the information