Firs Primary School

E-Safety Policy

Date written:	**November 2016**
Revised:	**February 2019**
	February 2020

Context

Firs Primary School recognises that there is a duty to ensure that all pupils are able to make a valuable contribution to society and this is only possible to achieve if we ensure that pupils develop and apply their computing capability effectively and safely in their everyday lives.

The school is aware of its responsibilities in ensuring that technology usage within school is responsible, safe and secure.

This E-safety policy is written to reflect the importance of using technology safety and how by doing this, pupils and staff can be protected. The policy raises awareness of the safety issues by providing clear guidance on how to minimise risks and how to deal with any infringements of school policy. The policy also identifies how to introduce the concept of E-safety to pupils.

What is E-safety?

E-safety encompasses internet technologies and electronic communications. It highlights the need to educate pupils about the benefits and risks of using technology and how users can safeguard their online experience.

"E-safety may be described as the school's ability: to protect and educate pupils and staff in their technology" and "to have the appropriate mechanisms to intervene and support any incident where appropriate" *Ofsted, 2014.*

Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and outside of school by children include:

- The internet
- Smart phones
- Digital cameras
- E-mail
- Instant messaging
- Web cams
- Blogs
- Podcasting
- Social networking sites
- Video broadcasting sites
- Chat rooms
- Gaming sites
- Game consoles

Roles and Responsibilities

This policy is responsibility of the computing co-ordinator and reflects to other policies including the anti-bullying policy and the safeguarding policy. The head teacher ensures that the policy is implemented and compliances with the policy will be monitored.

All teachers are responsible for promoting safe behaviours in their classrooms and following school procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bulling, abuse or inappropriate materials.

All staff should be familiar with the policy including:

- Safe use of e-mail;
- Safe use of the internet including social media;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobiles phones and digital cameras;
- Publication of pupil information/photographs and use of the website;
- Cyberbullying procedures
- Their role in providing E-Safety education for pupils.

The school includes E-Safety in their computing curriculum and ensure that every pupils has been educated about safe and responsible use. All classes teach e-safety the first week of every half term as pupils need to know how to control and minimise online risks and how to report a problem.

"In the five schools where provision for e-safety was outstanding, all the staff, including members of the wider workforce, shared responsibility for it. Assemblies, tutorial time, personal, social, health and education lessons, and age appropriate curriculum for e-safety helped pupils to become safe and responsible users of new technologies" *Ofsted, 2014.*

Communications

How will the policy be introduced to pupils?

Many pupils are very familiar with the culture of new technologies. Pupils' perceptions of the risks are not always mature and hence; e-safety rules are explained or discussed in an age appropriate manner. Children will also take part in 'Safer Internet Day' and some children will become Digital Leaders.

To teach E-safety the school uses the slogan 'Zip it, Flag it Block it' which is outlined clearly by Child Alert.

http://www.childalert.co.uk/article.php?articles_id=26

Other resources that teachers can use to support the teaching of E-safety:

http://www.kidsmart.org.uk/
https://www.thinkuknow.co.uk/
http://www.bbc.co.uk/cbbc/curations/stay-safe
Video Lee & Kim: https://docs.google.com/file/d/0B-xy4V542OOITEdsWWhEdlBqMDQ/view
Video Safer Internet Day: https://docs.google.com/file/d/0B-xy4V542OOIa0ZLaUtLaUtXU0k/view

Smart Crew: http://www.childnet.com/resources/the-adventures-of-kara-winston-and-the-smart-crew

How will the policy be discussed with staff?

Staff will be given a copy of the e-safety policy to review and any training in safe and responsible internet use can be provided when required.

How will parents' support be enlisted?

Internet use in pupils' homes is an everyday activity. Unless parents are aware of the dangers, pupils may have unrestricted access to the internet. The school is able to help parents plan appropriate supervised use of the internet at home when requested.

Any issues that have arisen within school which relates to internet usages will be handled sensitively and parents will be advised accordingly. The e-safety policy will be also published onto the website.

How will complaints regarding E-Safety be handled?

The school will take all reasonable precautions to ensure E-safety. However owing to the international scaled and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or device. Neither the school nor the local authority can accept liability for material accessed, or any consequences of internet access.

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 the school safeguarding policy.

Complaints of cyberbullying are dealt with in accordance with our anti-bullying policy.

Managing the Internet Safely

The risks

The internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with restriction. These features of the internet make it both an invaluable resources used by millions of people every day as well as a potential risk to young and vulnerable people, as much of the material on the internet is published for an adult audience and some is unsuitable for pupils.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a 'No Blame' supportive culture if pupils are to report abuse.

Technical and Infrastructure

This school maintains a filtered internet connectivity which ensures that any websites that are inappropriate are blocked immediately. Both children and staff are aware that the internet is filtered and can be monitored and understand that they must report any failure of the filtering. If any material is suspected to be illegal the school will immediately refer this to the appropriate authorities.

Education and Training

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher/responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures pupils know what to do if they find inappropriate web material
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report abuse
- Teaches E-safety as part of the computing curriculum in line with the National Curriculum including:
    - To understand why online friends may not be who they say they are and to be careful in online environments;
    - To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings;

- To understand why they must not post pictures of videos of others without their permissions;
- To have strategies for dealing with receipt of inappropriate materials.

Managing Internet Access- Email

Email is now an essential means of communication for staff in our schools and increasingly for pupils and homes.

This school does not publish personal emails of pupils or staff on the school website. Staff must use only their provided school emails when signing up to websites and sending e-mails relating to school.

Pupils may only use approved email accounts on the school systems and through the learning platform.

The learning platform flags up any abusive emails sent from pupil's accounts and these are reported to the teacher.

Pupils must immediately tell a teacher if they receive an offensive email.

Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.

E-mails sent to external organisations should be written carefully.

Managing Internet Access- Digital Images

The headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.

Uploading of information is restricted to the website team. Class teachers must only edit their delegated page of the website.

Photographs published on the school website are only of those children who have had permission for this and do not have full names attached.

Photographs taken by anyone in school are only taken by school equipment and can only be stored and accessed on schools devices.

Managing Internet Access- Social Media

Parents and teachers need to be aware that the internet has emerging spaces and social networks which allow individuals to publish unmediated content. Social networking sits can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave

comments, over which there may be limited control. Pupils should be made aware of the age restrictions on the use of these websites and therefore schools should emphasise that the use of social media is inappropriate, but also be taught how accessible personal data can be and who it is shared to once it has been published.

Managing Equipment

The computer system/network is owned by the school and is made available to pupils to further their educations and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet or email activity on the network.

To ensure the network is used safely this school:

- Has set-up the network with a shared work area for pupils and a separate one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using individual user logins.

School Social Media Accounts - Staff

YouTube

Firs Primary has a YouTube account linked to an unused email address within the school domain. The YouTube account can be accessed by any member of staff to upload videos to promote our school. One member of staff to take control of the account by being the recovery email. Before uploading videos to YouTube staff will inform parents in a written letter of their intentions and provide the opportunity for any parents to respond. Staff will also ensure that the only children to be shown in the videos are those with image publication consent. With the videos, no last names of the children will be published. All videos uploaded will be made public but the comments and ratings will be turned off.

Twitter & Facebook

The aim of the school twitter and Facebook account is to share learning experiences across the school and important information. The school twitter Facebook account will be linked to an unused email address within the school

domain. The twitter account will be public to allow for re-tweets. The Twitter feed will also be published to the school website. The Twitter and Facebook account can be accessed by any member of staff to upload examples of work, tweets about their memorable experiences etc. When sending tweets or publishing posts, staff will ensure that no last names of children will be published. One member of staff has control of the accounts by being the recovery email. The computing lead, with the support of the safeguarding manager, will have responsibility in checking that the account is being used appropriately.

All parents will be informed of the Facebook and twitter account and be given the opportunity to withdraw from their child's photo or work being published on the account. Any withdrawals will be documented and shared with all members of staff. Parents will be encouraged to follow the school Twitter and/or Facebook account but will be asked that it is not used as a way of contacting the school with queries. Parents will also be reminded that it is not appropriate to attempt to find and follow/friend members of staff on social media. Staff are asked not to reply to any query tweets and not follow or associate their personal twitter account to the school twitter account.

Care must be taken to ensure any tweets to other twitter accounts must reflect well on the school, be professional and be with the vision of sharing and promoting educational experiences. This may be tweeting accounts of visitors into school, authors, book publishers, charities and school trip locations.

Any inappropriate comments left on the twitter account should immediately be removed and reported to the headteacher.

Safeguarding Actions – Staff

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

In case of child pornography being found, the member of staff should be immediately suspended and the police should be called: anyone may report any inappropriate or potentially illegal activity or abuse towards a child online to the Child Exploitation and Online Protection (CEOP).

All staff will be asked to sign to say that they have read and understood the E-safety policy.

Staff signing sheet
E-Safety Policy

Print Name	Please sign to say you have received a copy of the “E-Safety Policy” and agree to adhere to it	Date

Staff signing sheet
E-Safety Policy

Print Name	Please sign to say you have received a copy of the “E-Safety Policy” and agree to adhere to it	Date

Staff signing sheet
E-Safety Policy

Print Name	Please sign to say you have received a copy of the “E-Safety Policy” and agree to adhere to it	Date