East Boldon Infant School

E Safety Policy

This e safety policy was approved by the Governing Body on:	**Insert Date: October 2018**
The implementation of this e safety policy will be monitored by:	**Miss Holt**
Monitoring will take place at regular intervals:	**Annually**
Reporting to the Governing Body at regular intervals:	**Annually**
The E safety policy will be reviewed annually or more regularly in the light of new developments in the use of technologies, threats to e safety or incidents that have taken place. The next review date will be:	**Insert date: October 2019**
Should serious e safety incidents take place the following external persons/agencies should be informed:	

The school will monitor the use of the policy using:

- **Logs of reported incidents produced through *e-safe* solution**
- **Internal monitoring data for network activity**

Our school uses a broadband solution through Durham County Council, procured through South Tyneside Council.
The filtering solution (smoothwall) is administered through the ICT in schools team.

All adult users of the school network and internet must read and understand the scope of this policy and then sign an acceptable use agreement before being allowed access to the school services. Pupil users will sign and agree to acceptable user rules and procedures appropriate to their age and understanding.

Unlawful and Illegal Use

All users agree to use the service for lawful purposes only and not to use the Service to send or receive materials or data, which is:

- in violation of any law or regulation
- which is defamatory, offensive, abusive, indecent, obscene
- which constitutes harassment
- is in breach of confidence, privacy, trade secrets
- is in breach of any third party Intellectual Property rights (including copyright)
- is in breach of any other rights or has any fraudulent purpose of effect.

You are prohibited from storing, distributing or transmitting or permitting the storage distribution or transmission (whether intentionally or otherwise) of, any unlawful material through the Service.
Examples of unlawful material include:

- direct threats of physical harm
- hardcore and child abuse images
- copyrighted, trademarked and other proprietary material used without proper authorisation

You may not post, upload or otherwise distribute or permit the posting, uploading or distribution (whether intentionally or otherwise) of copyrighted material on our servers without the consent of the copyright holder. You must give acknowledgement to the source wherever such material is used.

In the event that the school, or council become aware of any breach of this clause, action may be taken. The storage, distribution, or transmission of unlawful materials could also lead to UK authorities alleging criminal liability. All school computers have forensic monitoring software provided by the e-safe and school receives weekly reports detailing any access to inappropriate websites. If more serious incidents are noted, the school will be informed urgently.

Violations of system or network security

Any violations of systems or network security are prohibited, and may result in the user facing criminal and civil liability. The school will investigate incidents involving such violations and will inform and co-operate with the relevant law enforcement organisations if a criminal violation is suspected. The user may be refused access to the network as a result of any breach of security. Violations may include, but are not limited to, the following:

- Unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network
- Unauthorised monitoring of data or traffic on any network or system without express authorisation of the owner of the system or network
- Interfering with any user, host or network including mail-bombing, flooding, and deliberate attempts to overload a system and broadcast attacks.

All machines connected to the schools network must have full up to date and appropriate virus protection. No user should try to remove or alter this software. Any violation will mean immediate removal of access.

Only approved devices will be connected to the school network. All users must log in to the school and no other method of access is permitted.

Passwords

Visitors to the network will also be given a user name and password. These will be rescinded when the visitor leaves. Access to the LAN will be granted at various levels deemed appropriate to the level of need of the user, i.e.: pupils, governors and parents will have differing needs and access levels to staff. Higher access levels are granted to administrator and technician.

Users should not share logins or passwords. Passwords should be changed regularly. All passwords should be complex in nature including capitals, lowercase, symbols and
numerals. The more complex the password the more protection you are providing. Passwords should be between 8-10 characters using single letters. A phrase password, which includes spaces, may be easier to remember.

All machines should be locked or logged out when unattended. Staff should also follow the policy of the school for security of the premises and equipment on it.

Pupils or staff leaving the school network

Logins will be cancelled and files should be transferred to the new teacher/school if appropriate.

Google drive and e mail accounts will be disabled within 1 week. The account will not be deleted so as useful documents can still be utilised by the school.

Shared Accounts –change any shared service passwords such as administrator accounts on servers, printers and network devices if necessary.
Service contracts and web sites where the employee is a named contact will need to be updated.

Video conferencing and weblinks

The school takes part in communications with other schools via video conferencing or dedicated websites. This must only be done with teacher supervision.

Uploading material

Designated staff have permission to upload photographs onto the school website and Twitter account. Staff must make sure that we have parental permission before uploading any photographs of children onto the school website. Photographs of children are not to be posted on out Twitter account but examples of work (where parents have agreed) can be posted. All users must remember that posted material represents the school and should not bring the school into disrepute.

Mobile Devices

If portable devices are brought into school to be used in teaching they must be approved by the Head Teacher and checked by the ICT Technician before being connected to the broadband network. Any portable devices brought into school, including mobile phones should have Bluetooth turned off.

Mobile devices must not be used to take photographs, video or sound clips of any child in the school. School devices must be used and photographs and video must be removed from the device as soon as possible and stored in the photo evidence file on the school shared area.

Any use of mobile technology to intimidate, bully, harass or threaten others will be counted as an infringement of network use. This may result in disconnection from the network or legal or civil disciplinary action. Uploading images and sound is only permissible if the subject involved gives permission.

Email Use

You must use the e-mail address issued by the school for employment purposes only.

You may not send e-mail to any user who does not wish to receive it. Users must refrain from sending further e-mail to a user after receiving a request to stop.

Chain letters, flood e-mails and mail bombs may not be propagated using the Service. You may not operate or assist in any way whatsoever any web site, email address, email service or any other online service, which is advertised or promoted by means of Unsolicited Bulk Email

You may not use false e-mail headers or alter the headers of e-mail messages to conceal their e-mail address or to prevent Internet users from responding to messages. You may not use any email address that you are not authorised to use.

E-mail sent through the school service is deemed to be representing the school. As such any e-mail must not contain defamatory remarks, offensive language or other inappropriate material.

Attachments may only be opened if you are certain they do not contain any virus or other damaging content.

Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Any digital communication between staff and parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

Whole class or group email addresses will be used at KS1. Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff. All content that is posted on the website must be approved by the Head Teacher.

World Wide Web usage

All access to the Internet is filtered via a Firewall and 'Cloud' filtering.

The school monitors internet sites visited and may prohibit access to some sites deemed unacceptable or inappropriate.

All Internet usage from the network is monitored and logged and a log is kept of all sites visited. When specific circumstances of abuse warrant it, individual web sessions will be investigated and traced to the relevant site and user account. Such an investigation may result in action and possibly criminal investigation.

The laws of all nation states, regulating such diverse subjects as intellectual property, fraud, defamation, pornography, insurance, banking, financial services and tax, apply equally to on-line activities.

Documents or material must not be published or accessed on the web which are defamatory or which may constitute intimidating, hostile or offensive material on the basis of sex, race, colour, religion, national origin, sexual orientation or disability under the sovereign law of the country in which the web server hosting the published material is sited.

Images

Any images that involve children must not identify children by name and permission must have been agreed by the subject and/or relevant parent / carer before posting. The photos should then be stored in a safe area within the school LAN and only used for legitimate educational purposes as directed by the Head Teacher.

Images must be downloaded from cameras/memory cards/mobile devices to a LAN secure shared area and stored in a clearly labelled folder. This must be done immediately. Original images on cameras or other devices must be deleted prior to it being taken off site.

Before using images in other media (e.g. email, online, paper based and other collateral) ensure permission given covers intended use.

Care should be taken when taking digital / video images that Pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Social Networking and Media

Pupils will take part in E-safety lessons that includes an introduction to safe messaging. Teachers will moderate social media tools such as blogs if used on the school network for learning purposes.

Staff are not permitted to access personal social media accounts in school. Whilst we appreciate staff may use social media outside of school they are constantly reminded that any social media used at home should not identify the school or any pupils and any work issues should not be discussed. Staff must act in a professional manner both inside and outside of school. Designated staff can access the school's Twitter account to post updates (see Uploading Material section).

Disciplinary and Related Action

The school wishes to promote the highest standards in relation to good practice and security in the use of information technology. Consequently it expects and supports the integrity of its users. The school system is monitored on a regular basis and any misuse is reported and followed through.

In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow. The school will also assist where necessary should an investigation be called for by the police.

All cases of inappropriate use are logged in the E-Safety Log, held in the Office. All cases of sites deemed inappropriate by the school and the action taken are also held on file.

Storage of Information

Digital images may only be stored on the staff shared area.

Access to inappropriate material and reporting

Should a pupil access a site that they deem to be inappropriate by accident they should inform the class teacher immediately who will inform the head teacher. Pupils should activate screening software immediately (Hector Protector). The site will be recorded in the e-safety log and filtering adjusted if necessary. Do not show anyone the content or make public the URL. If reporting a URL do not copy and paste, type the address. The site will then be reported to the LA.

Should a user discover deliberate misuse or abuse or is the victim of cyber-bullying they should inform the Head Teacher. All incidents will be recorded in the e-safety log and acted on.

Users must report and a log made of all e safety concerns such as access to inappropriate sites, unacceptable e mail and any instances of cyber bullying. The report will be made to the Head Teacher who will then decide whether the incident should be progressed further in accordance with guidance issued by the LA.

Use of school equipment

School laptops and equipment should only be used by the nominated school employee and for educational use only.

E Safety Education

Pupils

Children will take part in planned E-safety lessons from Reception to Year 2. Children will be made aware of the procedures in place if they access any material they think is inappropriate. This information will be displayed next to the computers in the classroom.

Parents / carers

The school will therefore seek to provide information and awareness to parents and carers through:
- Letters, newsletters, web site, Twitter
- Parents evenings

Staff

It is essential that all staff receive e-safety training and understand their responsibilities. Training will be offered as follows:
• A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
• All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
• The Head Teacher (or other nominated person) will receive regular updates through attendance at training sessions run by the LA and external sources.
• This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
• The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training as required to individuals as required

Governors

There is a designated e-safety governor who has accessed training to the appropriate level.
• Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation is recommended
• Participation in school training / information sessions for staff or parents
• GEL – access to online training.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures are implemented.

- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- Remote management tools are used by technical staff to control workstations and view user's activity.
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Head Teacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.