INGLEBY MILL PRIMARY SCHOOL

POLICY FOR
E-Safety

December 2019

Les Rix
Due to be reviewed December 2022

School E-Safety Policy

IMPS has appointed E-Safety Coordinator, Mr L.Rix (Computing Subject Leader). The Designated Safeguarding Lead is Mrs B.Atkinson (Headteacher). Mrs K.Coverdale and Mrs A. Dent are designated Safeguarding Officers.

Our E-Safety Policy has been written by the school and seeks to incorporate the current government guidance. It has been agreed by the senior leadership team and has been recently approved by the school governing body in November 2019.

The E-Safety Policy for Ingleby Mill Primary School will be reviewed every two years. This policy will next be reviewed in September 2021.

Why is Internet Use Important at Ingleby Mill?

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 information and administration systems.

Internet use is part of the statutory curriculum and is a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

We accept that pupils will use the internet outside school and will therefore need to learn, inside school, how to evaluate internet information and how to take care of their own safety and security.

How does Internet Use Benefit Education?

<u>Benefits of using the internet in education include:</u>

- access to world-wide educational resources including encyclopedias online resources, educational movies news updates;

- inclusion in the National Education Network which connects all UK schools;

- educational and cultural exchanges between pupils world-wide;

- access to experts in many fields for pupils and staff;

- professional development for staff through access to national developments, educational materials and effective curriculum practice;

- collaboration across support services and professional associations;
- improved access to technical support including remote management
- exchange of curriculum and administration data with the Local Authority and DFE; access to learning wherever and whenever convenient.

How can internet use Enhance Learning?

- The school internet access will be designed expressly for pupil use and includes Smoothwall filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff will be expected to guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised internet access.
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web Protocol

- If staff or pupils discover unsuitable sites, the URL (address), time, content etc must be reported to the network management One IT via the E-safety coordinator or network manager.
- A record of E-Safety incidents is kept on CPOMS noting the incident, who was involved and the action taken and is maintained by all staff.

- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.

- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Online behaviour

School will enable pupils to understand what acceptable and unacceptable online behaviour look like. School will teach pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. School will also teach pupils to recognise unacceptable behaviour in others.

Schools can help pupils to recognise acceptable and unacceptable behaviour by:

- looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do,

- looking at how online emotions can be intensified

- teaching techniques (relevant on and offline) to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online; and

- considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

Use of Email

- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts for pupils will be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters and virals is not permitted.

Social Networking

- School will endeavour to block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils will be taught about the importance of e-security and encouraged to always set passwords, deny access to unknown individuals and will be instructed how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others.

Filtering

The school will work in partnership with One IT (Smoothwall) and the Internet Service Provider to ensure filtering systems are as effective as possible.

Managing Emerging Technologies/Use of Mobile Devices

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

- Mobile phones for both staff and pupils will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

- Staff may use a mobile phone at break/dinnertime only and must seek an area of privacy to make the call – such as the staffroom.

- Any mobile device must be checked for viruses and spam content before being attached to the school network.

- Mobile devices must not be used to take photographs or sound clips of any person who is unaware of the action and who has not given their permission.

- 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.

- Any images that involve children must not identify children by name and permission must have been agreed by the relevant parent / carer before posting. A record should be made of who will be taking the photos, why the photos are being taken, when they are being taken and what they are to be used for. This should all be documented in the risk assessment carried out before a school trip or event. The photos should then be stored in a safe area within the school local authority network and only used for legitimate educational purposes as directed by the Headteacher.

- Photographs taken by Foundation Stage staff for use in observation and assessment will remain only on the school network.

- It is understood that at times EYFS practitioners maybe completing photographic assessments offsite and these are only to be used through Target Tracker. Under any circumstances, images must not be stored on their own personal computers.

- **Laptops**

Laptops for teachers are the property of the school and should be treated like any other school computer.

- The user is responsible for ensuring the privacy and security of data held on any laptop and for ensuring the integrity of such data by keeping antivirus software up to date, as a minimum.

- The laptop should not be used by third parties or family members. It should not be loaned out to third parties. It should be keep in a secure location at all times, whether on or off the school site.

- Connection of the laptop to the Internet makes it highly susceptible to interference from outside and this should be borne in mind when using it to browse the web. Laptops containing sensitive pupil data can easily be compromised by connection to any network, but particularly to the Internet, and this data cold be procured by any third party via an Internet connection or perhaps a home wireless network.

- School laptops should not be connected to a third party wireless broadband connection without that party's knowledge and/or permission. Doing so is a very serious matter and could lead to civil action.

- Laptops brought into school for repair by technicians will be subject to scrutiny if found to contain any virus or suspicious software or document, including dubious images. Any unsuitable content or usage discovered will be reported to the Headteacher in the first instance.

- Peer to peer software (P2P) must not be installed on any laptop e.g. any file sharing websites (music, films, images etc)

- The school reserves the right to audit any school laptop on demand and report any findings related to misuse e.g. pornography or illegal software, to the relevant authority.

- Staff who terminate their employment or are on long term sick leave should return their laptop to the School ensuring that any personal data has been backed up and or removed.

- Staff should not remove a laptop from the school building unless they have signed the school Laptop Policy and all equipment must be signed in and out of the building.

Protecting Computers from Theft

- All computer equipment is security marked

- Charging cabinets are locked securely each night and are the responsibility of the Team Leader or a designated staff who they choose.

- Teacher in charge checks equipment at the end of each lesson and makes sure users are logged off and equipment shut down.

- Borrowing Hardware – Any member of staff wishing to borrow a computer for use at home during school time will need to follow the school procedures and obtain permission from the School Business Manager and once approved, sign the computer out in the school office.

Published Content and the School Web Site

The contact details on the school website will be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

The head teacher and nominees – J.Measor (School Business Manager), will take overall editorial responsibility and ensure that content is accurate and appropriate. Web content management system (CMS) is provided by One IT of Stockton.

Publishing Pupils' Images and Work

- Photographs that include pupils from Ingleby Mill will be selected carefully and will not enable individual pupils to be clearly identified without parent consent

- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs without parent consent

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.

- Work can only be published with the permission of the pupil and parents/carers.

Information System Security

- School ICT systems capacity and security will be reviewed regularly by the Computing Subject Leader and Subject Leader Group.

- Virus protection will be installed and updated regularly by the Local Authority and Network Management from One IT.

- Security strategies will be discussed with the Local Authority and the Head-teacher.

Protecting Personal Data

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

Assessing Risks

The online world develops and changes at great speed. New opportunities, challenges and risks are appearing all the time. This can make it difficult for schools to stay up to date with the latest devices, platforms, apps, trends and related threats.

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Stockton-on-Tees Borough Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and will report as necessary to the Headteacher.

Staff will be updated on:

Age restrictions - Some online activities have age restrictions because they include content which is not appropriate for children under a specific age.

Content: How it can be used and shared - Knowing what happens to information, comments or images that are put online.

Disinformation, misinformation and hoaxes - Some information shared online is accidentally or intentionally wrong, misleading, or exaggerated.

Fake websites and scam emails - Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other gain.

Fraud (online) - Fraud can take place online and can have serious consequences for individuals and organisations.

Password phishing - Password phishing is the process by which people try to find out your passwords so they can access protected content.

Personal data - Online platforms and search engines gather personal data. This is often referred to as ‘harvesting’ or ‘farming’.

Privacy settings - Almost all devices, websites, apps and other online services come with privacy setting that can be used to control what is shared.

Handling E-Safety Complaints

- Complaints of Internet misuse by pupils will be dealt with by the Computing Subject Leader and the Headteacher. The class teacher involved will also report to parents.
- Any complaint about staff misuse must be referred directly to the Headteacher.
- Complaints of a child protection nature must be always dealt with in accordance with school child protection procedures. (Guidance is available, published 2016, to staff in assessing risk and the management of 'sexting' concerns or other inappropriate use)
- Pupils and parents/carers will be informed of the complaints procedure.
- A record of E-Safety incidents is kept on CPOMS noting the incident, who was involved and the action taken and is maintained by all staff.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all key areas.
- Pupils will be informed that Internet use will be monitored.

Staff

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents / Carers

Parents' / carers' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school website.

E-Safety Rules

These E-safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network access or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and internet use must be appropriate and related to an educational purpose.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as e-mail could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the Head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or unspecified illegal purposes is not permitted.

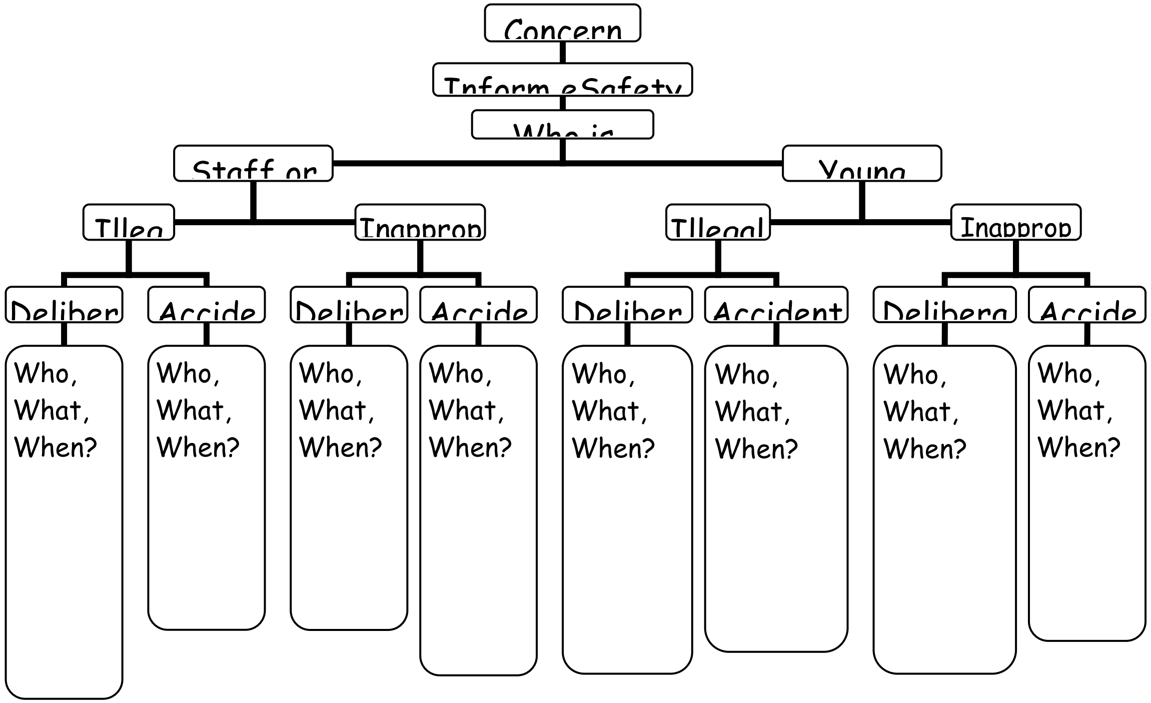
The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Ingleby Mill Primary School

Rules for Responsible Internet Use

The school has computers with Internet Access to help our learning.
Follow these rules to keep you safe and help us be fair to others.

- I **will** only access the school network with my own login and password which I will keep secret
- I **will not** access other people's files
- I **will not** bring in or use memory sticks from outside school unless I have been given permission and had it virus checked by a teacher
- I **will** ask permission from a member of staff before using the internet
- I **will** only e-mail people I know, or who my teacher has approved
- The messages I send will be **polite** and **responsible**
- I **will not** give my home address or telephone number to anyone
- I **will not** arrange to meet anyone following an e-mail
- I **will** report any unpleasant material or messages sent to me. This report will be made confidentially and would help protect other pupils and myself
- I **understand** that the school may check my computer files at **any time** and monitor the Internet sites that I visit.


Concern
Inform eSafety
Who is
Staff or
Young
Illeg
Inapprop
Illegal
Inapprop
Deliber
Accide
Deliber
Accide
Deliber
Accident
Delibera
Accide
Who, What, When?
Who, What, When?
Who, What, When?
Who, What, When?
Who, What, When?
Who, What, When?
Who, What, When?
Who, What, When?