FIRTHMOOR PRIMARY SCHOOL

Online Safety and ICT Policy

Date policy approved	October 22
Review frequency	Annual
Review date	October 23

This policy should be considered alongside other related policies within the school. Other related policies are:

Health and Safety
Child Protection and Safeguarding
Protect and Prevent (Extremism and Radicalisation) Policy
Mobile Phone Use
Code of Conduct
Anti-Bullying Policy
Behaviour Policy
PSHE Policy
Data Protection Polices and Procedures (GDPR)

Introduction

All members of school/setting communities have an essential role to play in ensuring the safety and wellbeing of others, both on and offline. These guidelines have been drawn up to ensure that all stakeholders within the school are aware of what is expected of them and are able to stay safe when using the hardware and software we have in school. The equipment and resources within school are provided to enhance the learning of the pupils and to aid the staff in their delivery of the curriculum; this policy will enable these to go ahead. It is important that all members of the community are aware of these roles and responsibilities and also how to access and seek support and guidance.

Aims

ICT encompasses every part of modern life and it is important that our children are taught how to use these tools and more importantly, how to use them safely. We believe that it is important for children, staff and the wider school community to have the confidence and ability to use these tools to prepare them for an ever-changing and rapidly developing world. To enable all our staff and pupils to be confident, competent independent users and learners of ICT
In our school we aim:

- To use ICT where appropriate to ensure pupils are motivated and inspired in all areas of the curriculum
- To use ICT to help improve standards in all subjects across the curriculum
- To develop the ICT competence and skills of pupils and provide them with the chance to consolidate these in a cross-curricular context
- To ensure pupils are challenged in their use of ICT and are provided with exciting, creative ways in which to share their learning
- To use tools available to ensure children have the ability to work independently and collaboratively to suit the needs of the situation
- To provide all staff with the training and support to ensure that they can, and have the confidence to, use ICT to its full potential in all aspects of school life
- To use ICT as a form of communication with parents, pupils and the wider community

Curriculum

ICT will be taught across the curriculum and wherever possible and appropriate, integrated into other subjects. There may be a need for stand-alone ICT sessions to teach skills that can then be applied in the cross-curricular sessions. Children may be taught ICT skills using computers in the classrooms, Ipads, Laptops, Chromebooks and Surface pros. In Reception, children will be taught how to use various pieces of ICT equipment which can include Ipads, programmable toys and class computers, in accordance to the Early Learning Goals appropriate for them.

We differentiate work in a variety of ways in order to ensure that all pupils are able to access the curriculum and make good progress. These include:

- presenting work to children using, and requiring use of, different learning styles
- same activity but different outcome;
- groupings of pupils;
- development of different modules of work for a range of abilities;
- different pace of working – including the use of extension activities;

Teachers ensure that opportunities are given to use a variety of equipment, in conjunction with the classroom computers, such as digital cameras, video cameras, portable devices and programmable vehicles. All the software used in school is monitored to ensure that its use is non-discriminatory, exciting and varied and represents cultural diversity.

Online Learning

As a school, we value the importance of providing opportunities for children to learn outside of school and we will provide these depending on the age of the child. On our website we provide links to generic websites such as My Maths and BBC Bitesize. We also provide pupils with logins for online tools such as Purple Mash, Google Education and Mathletics.

Roles and Responsibilities – Online Safety

The headteacher has overall responsibility for the management of all aspects of ICT, training and online safety throughout the school. All staff have a responsibility to ensure that internet access is safe and appropriate. They will have access to the Schools Online and ICT Policy, which includes all aspects of E-Safety, and its importance explained. Staff should be aware that Internet traffic could be monitored and that discretion and professional conduct is essential.

The measures outlined below are designed to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the Internet.

- Internet access includes a “firewall” filtering system intended to prevent access to material inappropriate for children. The system used is Netsweeper Education and is provided by and monitored through our Broadband provider, Talk Straight.
- Children using the Internet will be working in the presence of the class teacher or other approved adult helper. Different levels of access are granted on the basis of pupil access or job role.
- Staff will check that sites pre-selected for children’s use are appropriate for their age and maturity and report any sites to either the SBM or ICT engineer that are not approved or deemed inappropriate

- Staff will be particularly vigilant when children are undertaking their own search and will ensure that they are following an agreed search plan.
- Children will be taught to use e-mail and the Internet responsibly in order to reduce the risk to themselves and others.
- Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils acceptable use and risks.
- Teachers will have access to pupils' emails and other Internet related files, and will check these on a regular basis to ensure expectations of behaviour are being met.
- Children will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable
- Pupils and Staff consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources. They will also come under the general discipline procedures of the school.
- Pupils and Staff should not access other people's files unless permission has been given.
- No program files may be downloaded to the computer from the Internet. This is to prevent corruption of data and avoid viruses.
- Uploading and downloading of non-approved software will not be permitted.
- There will be no access to social networking/gaming from school equipment.
- The school will deny access to social networking sites and students will be advised not to use these at home.
- Staff and Pupils must not share their usernames or passwords with anyone.

Internet access and home/school links

- Parents will be informed in the school prospectus that children are provided with supervised Internet access as part of their lessons and will be kept informed of future developments by letter and newsletter.
- Parents and children will be expected to sign a permission form before they begin using the Internet to share responsibility with the school.
- Parents are required to inform the school by a permission form, if they have any objections to their child's work or photographs being published. If the parent has not specified a wish for their child to be excluded it will be assumed we have the parents' permission

School Website

- The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- The publication of children's work will be at the decision of the class teacher**.**
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- The school will ensure that the image files are appropriately named and will not use pupils' names in image file names if published on the web.

School and personal social media usage

To enhance communication, parental engagement and promotion of the school and its activities, Firthmoor Primary school currently manages both a Facebook and Twitter account. Both of these accounts have the appropriate privacy and restricted settings and are managed by a small number of staff with admin access rights. Staff are reminded that these social media sites are for school related activities and not to be used for any personal gain or to resolve disputes. Other related school policies restrict the use of personal social media accounts whilst on school site.

In relation to personal social media accounts, and in line with the school's code of conduct, staff are reminded to:

- Not accept friend requests from current pupils or ex-pupils under the age of 18
- Notify the school's DSL if a child sends a friend request
- Use extreme caution when corresponding with parents via social media, and use a school email address instead
- Not discuss anything to do with school, pupils or other staff members, or post photos of school events on their private accounts. School activities are to be communicated via the school social media sites
- Only post things that they would be happy to be attributed to them as a teaching professional
- Not identify themselves as being associated with the school
- Use the tightest privacy settings possible
- Not use social media on school devices and only use personal devices within designated areas as per the School's Mobile Phone and Portable Devices policy

Parents are reminded to:

- Not post photos, videos or comments that include other children at the school
- Not use social media on their own devices while on school premises
- Not access social media while helping at school or on school visits
- Raise queries, concerns and complaints directly with the school rather than posting them on social media – whether on their own pages, in closed groups (e.g. groups set up for school parents to communicate with each other) or on the school's pages
- Not post anything malicious about the school or any member of the school community and to raise any concerns direct to the headteacher or governing body

Children are reminded to:

- Not join any social networking sites if they are below the permitted age (13 for most sites including Facebook and Instagram)
- Tell their parents if they are using the sites, and when they are online
- Be aware of how to report abuse and inappropriate content
- Not access social media on school devices, or on their own devices while they're at school
- Not make inappropriate comments (including in private messages) about the school, teachers or other children

Reporting incidences
The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the scale and nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

Should an incident occur in which children are exposed to offensive or upsetting material, the school will respond to the situation quickly. The Headteacher will deal with complaints of Internet misuse.

- Any complaint about staff misuse must be referred to the Headteacher (DSL) or Deputy Safeguarding Lead.
- Methods to quantify and minimise the risk of children being exposed to inappropriate material will be reviewed.
- Where necessary, the children's parents will be informed and given an explanation of the course of action taken.
- The ICT Co-ordinator or SBM will report the URL (address) and content of unsuitable sites to the Internet service provider and the IT Technician.
- Complaints of a child protection nature must be dealt with in accordance with school Safeguarding and Child Protection Procedures

Technical – Infrastructure / equipment, filtering and monitoring
The school network is managed by the IT technician through an SLA. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure.

- School technical systems will be managed to that ensure that the school meets recommended technical requirements
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to schools technical systems and devices.
- The SBM and IT technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users and is monitored. Users must agree and sign an Acceptable Use Agreement *(Appendix 1 & 2)*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed procedure is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Portable Equipment and Devices
The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. However, there are a number of e-safety considerations for portable devices that need to be reviewed. Considerations include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during school time.
- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the General Data Protection Regulation (GDPR) principles
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's / academy's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Pupils receive training and guidance on the use of portable devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device lost, stolen or change of ownership of the device will be reported to the SBM
- Any devices on loan, must be logged in the Equipment on Loan register

Use of digital and video images

Staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may remain available on the internet forever and could possibly be used to cause harm or embarrassment to individuals in the short or longer term. The school aims to inform and educate users about these risks.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (eg on social networking sites)
- Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by GDPR). However, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff / volunteers or visitors should not be used for such purposes. Mobile phones must not be used within school hours or used to take pictures/videos of pupil's work. Mobile devices, such as Ipads, Surface Pro's, must not be used to take photographs, video or sound clips of any person who is unaware of the action and who has not given their permission.
- The school will provide an IPad to record and take pictures during off site activities. This device must be signed for when used and is pin protected. Data stored on the device must be downloaded to the school's network upon return.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers will be obtained before photographs and work of students / pupils are published for either the school website or for promotional purposes of the school.

Data Protection (GDPR)
All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Firthmoor Primary School's policies and procedures are designed to ensure compliance with the principles. Personal data will be recorded, processed, transferred and made available according to the GDPR which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection**.**

The school will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy (GDPR Statement)
- It is registered as a Data Controller for the purposes of the GDPR
- Risk assessments and checks are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

All staff and visitors must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session or "computer locked" when they are away from their computer in which they are using personal data.
- Transfer data using encryption and secure password protected devices and software
- Report any breaches, faults or loss of data to the headteacher or SBM

Monitoring and review
The policy will be reviewed every two years, or earlier in the light of any changed circumstances, either in our school or current legislation

Firthmoor Primary School
Rules for Responsible Internet Use

PUPILS

The school has computers and internet access to help our learning. These rules will help keep everyone safe and be fair to others.

- I will only access email and the computer with my own log-in and password details, which I will keep secret from everyone else.
- I will not access other people's files.
- I will only use the computers for school work and homework.
- I will not bring CD's or memory USB memory sticks into school from home.
- I will ask permission from a member of staff before using the Internet.
- I will only email people I know or people that my teacher has approved.
- I will only access internet sites that my teacher has approved.
- The messages I send will be polite and sensible.

I will not give out any of my personal details, such as home address, telephone number, email address or personal website details, nor will I arrange to meet someone, unless my parent, carer or teacher has given permission.

To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like.

I understand that the school may check my computer files and monitor the websites I visit.

PUPILS AGREEMENT

I agree to follow the rules for Responsible Internet Use.

Signed_____

Print name_____

Class_____Date_____

Dear Parents/Carers,

Responsible Internet Use

As part of pupils' curriculum enhancement and the development of ICT skills, Firthmoor Primary School is providing supervised access to the Internet, including email.

Our school Internet access provider operates a filtering system that restricts access to inappropriate materials.

The access your child will have to the Internet will be planned and appropriate to their educational needs. On the front of this sheet, there is a list of the Rules for Responsible Internet Use that we operate at Firthmoor Primary School.

Should you wish to discuss any aspect of Internet use, please telephone the school to arrange an appointment.

Parents are requested to complete the school's parental consent form which includes the online safety agreement and permission for your child to access the internet and online tools, such as Gmail and Google Education, for their work in school.

FIRTHMOOR PRIMARY SCHOOL
ACCEPTABLE USE POLICY

This Acceptable Use Policy covers the security and use of all Firthmoor Primary School's information and IT equipment. It also includes the use of email, internet, voice, mobile and portable IT equipment. This policy applies to all Firthmoor Primary School employees, pupils, contractors and stakeholders.

Computer Access Control - Individual's Responsibility
Access to Firthmoor Prima ry School's IT system is controlled by the use of user IDs and passwords. All user IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the school's IT systems.

It is strongly recommended that passwords are changed regularly and where possible, contain letters, characters and numbers. Passwords and user IDs are not to be shared. If passwords are written down, they MUST NOT be displayed in public view and must be recorded and locked away securely

Email Use
Use of the schools internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance; is not detrimental to Firthmoor Primary School in any way; is not in breach of any terms and conditions of employment and it does not place the individual or Firthmoor Primary School in breach of any statutory or other legal obligations.

You may not send email to any user who does not wish to receive it or use any email address you are not authorised to use.

The school email system and accounts must never be registered or subscribed to spam or other non-work-related updates, advertisements or other personal communications. School email addresses must not be shared without confirming that they will not be subjected to SPAM or sold on to marketing companies

You may not use the internet or email to make personal gains or conduct a personal business.

You must not send unprotected sensitive or confidential information externally.

Inappropriate Use
Accessing or having possession of offensive material of any level or content of an obscene, indecent and/or abusive nature could result in a disciplinary and/or civil action.

You must not:
Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
In any way infringe any copyright, database rights, trademarks or other intellectual property.
Download any software from the internet without prior approval of the IT Department.

Monitoring and Reporting
Logs may be kept of sites visited. Any violations identified may result in further investigation and criminal/disciplinary action.

Violations of system or network security
Computers and equipment will be disconnected if security is violated. Any equipment connected to Firthmoor Primary School's network must access the internet through an approved security / web filtering appliance.

Any equipment connected to the school's network must have full up to date and appropriate anti-virus and anti-spam protection.

Any machine infecting the network must immediately be disconnected, cleaned and not reconnected to the network until it has been fully checked by the school's IT engineer.

Unauthorised Use
Staff are not permitted, under any circumstances, to:

- Use the ICT facilities for commercial or financial gain
- Relocate, take off-site, or otherwise interfere with the ICT facilities without the authorisation of the ICT technician or headteacher.
- Use or attempt to use someone else's user account. All users of the ICT facilities will be issued with a unique user account and password. The password must be changed at regular intervals. User account passwords must never be disclosed to or by anyone
- Use the ICT facilities at any time to access, download, send, receive, view or display any of the following:
    - Any material that is illegal
    - Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
    - Online gambling
    - Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
    - Any sexually explicit content, or adult or chat-line phone numbers
- Generate messages or documents that appear to originate from someone else
- Install hardware or software without prior consent from the ICT technician or headteacher
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the school's computers.
- Knowingly distribute a virus or harmful code to the school's network
- Use or attempt to use the school's ICT facilities for illegal activity such as piracy or copyright provisions
- Use the ICT facilities and network to send confidential information and data to unauthorised parties. Data will only be shared for relevant processing purposes

- Be wasteful of ICT resources, such as toners, ink and paper
- Use the iCT facilities when it will interfere with your responsibilities
- Operate equipment to record an image beneath a person's clothing with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks without their knowledge or consent (whether exposed or covered by underwear) – otherwise known as "upskirting".

Any unauthorised use of the school's ICT facilities is likely to result in disciplinary action

Loan Equipment

School equipment, including electronic devices may be loaned to staff. Devices must be logged within the loan register, detailing the length of time the loan request is for. Devices on loan are encrypted and protected to ensure the security of data. Staff are made aware that a replacement fee may be charges if any loss or damage is incurred whilst the device is on loan

Social Media
Access to social media is limited to a restricted number of staff to ensure all members of the school community are kept safe. Staff are reminded to uses the tightest privacy settings on their social media pages.

Taking and storing images
Strong passwords / PIN numbers must be used with all portable equipment

Images that involve children should not identify children by name, or by first name only and permission should have been agreed by the subject and/or relevant parent / carer before posting. Mobile devices belonging to the school may be used to take photographs, video or sound clips of any person, but must not be used if the person is unaware of the action and has not given their permission. **All media must be removed from the device and saved onto the school network as soon as possible**

Mobile phones or personal devices must not be used to take photographs, audio or video clips.

Data handling and data transfer
All data referring to individuals or that contains sensitive information MUST be encrypted and stored securely

Reporting Accidental Access to inappropriate material and / or Deliberate Misuse
Any user who comes across inappropriate or offensive material should inform the website address to the Headteacher, SBM or IT technician who will request a log of the web address, time and username in the incident log. The IT technician will block the site to restrict access.

Confirmation of access to illegal materials or the committing of illegal acts will be reported to the relevant police authority for investigation.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, Firthmoor Primary School advises a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All confidential related material must be disposed of using confidential waste bins or shredders.
- General housekeeping and removal of documents is advised. It is recommended to remove any unnecessary documents on an annual basis or earlier if necessary (Data Protection)

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Equipment and paperwork taken off-site must not be left unattended in public places and not left in sight in a car.
- Information should be protected against loss or compromise when working remotely
- Laptop and mobile devices (USB pen drives, IPads) containing sensitive data must be encrypted.
- Equipment belonging to the school must be logged and signed for
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Employee Name:

Signature:

Date: