The Meadows Primary School
Acceptable Use Policy

Introduction

This policy should be read alongside the safeguarding policy and whole-school curriculum intent statement.

The internet is an essential element of 21st Century life for education and social interaction. The purpose of internet use in school is to support pupil achievement, to facilitate the professional work of staff and to enhance the school's management, information and business administration systems.

Benefits include:

- Access to worldwide resources and research materials
- Educational and cultural exchanges worldwide
- Access to experts in many fields
- Staff professional development such as access to online learning and forums
- Communication with support services, professional associations and colleagues
- Exchange of curricular and administration data (i.e. between colleagues, LA and DfE)

The National Curriculum for computing requires pupils to learn how to become competent, safe and responsible users of computer technology. Consequently, in delivering the curriculum, teachers need to plan to integrate the use of IT and web-based resources, that may include email, to enrich learning activities. Effective internet use is an essential life-skill.

Access to the school's network and use of IT facilities owned by the school, including access to the internet, are conditional on observance of the following Acceptable Use Policy.

The aims of this Acceptable Use Policy are to:

- Allow all users access to school IT resources and use of the internet for educational and administrative purposes, as is appropriate for their role.
- Provide a mechanism by which staff and pupils are protected from internet sites, information, and individuals that would undermine or harm both them and the school.
- Provide rules which are consistent, and in agreement with the Data Protection Act 2018, Computer Misuse Act 1990 and other legislation relevant to the use of IT and electronic data in schools.
- Provide rules relating to the use of computers and IT facilities in school, which are consistent with the general policies of the school.

General network, internet use and consent

Pupils who are to have access to the school's computer network and internet must understand the basic conventions and navigation techniques before going online and accessing material. This will be taught in class sessions at an age-appropriate level. Pupils must not use the school IT facilities without supervision of a member of staff. Computer facilities and access to the internet will be supervised, and all possible measures will be taken to ensure that children are only able to access age-appropriate content. The internet is subject to a high level of content-filtering and a firewall to prevent access to inappropriate material. It is managed by F1 Group. However, The Meadows Primary School cannot accept liability for the accessing of inappropriate materials or any consequences of internet access.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to a member of the senior leadership team or F1 computer technician who will record the address and report it to our provider, F1 Group.
Pupils are aware that they must only access those services they have been given permission to use.
Staff and pupils are made aware that the use of IT systems without permission or for inappropriate purpose is a criminal offence (Computer Misuse Act 1990).

Log in and passwords

- Staff must not disclose any password or login name, or allow anyone else to use their own personal account.
- Staff must not allow children to access the school network via the staff member's own login and password.
- Pupils log in to the school network using a generic username and password. They have access to a shared drive, where work may be stored. They do not have access to any of the other shared drives (see below).
- Pupils and staff must not attempt to gain access to the school network or any internet resource by using someone else's account name or password.
- Staff and pupils must ensure PCs and laptops are logged off when left unattended. Staff laptops must be logged off after use and at the close of the school day.
- Staff network passwords are set for each user. Passwords should be over 4 characters and should contain letters, numbers and symbols. Staff are encouraged to change them regularly and reminded to keep them private.
- Staff members have separate passwords for accessing the cloud-based Office 365 drive. Passwords for these accounts should also contain letters, numbers and symbols, and they should be changed regularly. They must be kept private.
- Only staff encrypted laptops may be taken off the school site and only Office 365 of the encrypted lap top's hard drive used to store any data, including documents. It is the responsibility of the member of staff to take all necessary steps to ensure the security of laptops taken off site. All other school and staff laptops and other IT devices (such as iPads) must remain on the school premises at all times, unless for use at an offsite school event- for example, a football tournament. The school office stores a central list of school devices and allocation details.

General safety and risk assessment

The consumption of food or drink is forbidden whilst using a computer. It is hazardous to the equipment and to individuals.
Users must treat school equipment and services, and other sites accessed via school devices, with respect. They are subject to regulations imposed by the respective service providers. Malicious action will result in immediate suspension from use of the school IT facilities.
Staff are responsible for sharing the safety issues with their pupils.

Cyber bullying

Bullying is defined as behaviour that is:

- intended to hurt someone either physically or emotionally
- repeated
- often aimed at certain groups, for example because of race, religion, gender or sexual-orientation

Cyberbullying is malicious and repeated behaviour that takes place online. Its effects are equally harmful, but its features may differ slightly:

- Through social media and online forums, cyberbullying can occur at any time and the perpetrator is 'invisible'
- The perpetrator may remain anonymous, or hide behind another identity
- The perpetrator can be any age and not known to the victim.

The experience of being cyberbullied can be very painful for those who are the targets.
Some instances of perceived malicious online behaviour may be unintentional: a message intended as a joke, for example: a comment with an ambiguous meaning; an email sent to the wrong recipient. This is why safe online behaviour is a crucial part of our curriculum. Adults need to help children prepare for the hazards of using technology while promoting learning and social opportunities.

Prevention

We recognise that the best way to deal with cyber bullying is to prevent it from happening in the first place. By embedding good, safe computer practice into all our teaching and learning, incidents can be avoided.
We recognise that we have a shared responsibility to prevent incidents of cyberbullying. Any incidents of cyberbullying will be addressed by following our safeguarding and bullying policies, and documented in line with this.

E-safety

Children and staff are taught about our acceptable use policy at an age-appropriate level, as part of classroom teaching. Any work or activity on the internet must be directly related to learning. E-safety lessons form part of our computing curriculum. We also access support and guidance from curriculum advisers and provide e-safety workshops for parents periodically.
Social-networking sites are not accessible via the school network.

Staff are strongly discouraged from accepting friend requests from parents on social-networking sites, and must never accept or initiate a friend request for a child in the school. Staff are reminded of the necessity to keep their profiles secure and to avoid contact with inappropriate persons (particularly parents/pupils or ex-pupils). Staff are reminded that any action or comment that brings the school or colleagues into disrepute or compromises pupil or staff confidentiality will be classed as a disciplinary matter.

Staff must not share any personal email or postal addresses or telephone numbers online – either their own information, or that of any members of staff or pupils with any other parties.
Staff and children must not download, use or upload any material that is copyright. If in doubt, or permission cannot be obtained, the material must not be used.

Users should assume that all software is subject to copyright restrictions. Pupils must not, under any circumstances, download or attempt to install any software on the school computers or network server. Staff should seek the advice of the senior leadership team and/or computer technician before attempting to download or upload software.

Under no circumstances should users view, upload or download any material that is likely to be unsuitable for children or schools. This applies to any material of violent, dangerous, racist or

pornographic content. If users are unsure about this, or any materials, users must seek advice from the computing/IT lead. If in doubt, they should be reminded that caution is the best policy and that no questionable materials should be accessed at any time. The transmission, storage, promotion or display of offensive, defamatory or harassing material is strictly forbidden as it breaches the laws of the UK under the Computer Misuse Act. Possession of certain types of unsuitable material can lead to prosecution by the police.

Photographs of pupils which will be featured on the website and/or Twitter require written consent from parents/carers, and this is updated annually. If a picture is placed on the school website or Twitter, the child's name is not displayed.

School network and file storage

General Drive (G:Drive)

The school network includes a general drive (G:Drive), where files are stored, and this can only be accessed via a staff login. Under no circumstances should children access this drive. It is not accessible via a pupil login. Staff must respect the privacy of files of other users in the G:Drive.

Shared Drive (S:Drive)

Pupils can save their work and access files using the shared drive (S:Drive). Children must not access the files of other students without permission. Staff and pupils must not modify or delete files of other user on any of the shared drives without obtaining permission from them first.

(W:Drive)

Senior leaders and school administrative staff can save work and access files using the W:Drive. This is not accessible via other staff or pupil logins. Other staff must not access, modify or delete the files of other users without obtaining permission from them first.

One Drive via Office 365

The Meadows Primary School has a subscription to Office 365, and files can be stored and shared securely on the associated One Drive. Staff are able to access this facility when working out of school. It is the responsibility of each member of staff to ensure that work is saved securely on One Drive and that open files are never left unattended on a PC, laptop of handheld device. Staff must log out of Office 365 and One Drive after each use, and before leaving a device.

The computing/IT subject leader will view any material pupils store on the school's computers. Storage space on the network is limited. All users are requested to ensure that old, unused files are removed from their area at the end of each academic year. Users unsure of what can be safely deleted should ask the computing/IT subject leader for advice.
Users accessing software or any services available through school facilities must comply with licence agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.

Seesaw

Seesaw is an online learning platform used by pupils and staff during school closures, and also for homework tasks weekly. It is a secure network, accessed by parents and carers using a username and password. Two staff administrators and the headteacher maintain an overview of the network. Pupils are asked to review the acceptable use policy before using the system and this is monitored by teachers and administrators. Pupils' work is only visible to their class teacher, the headteacher and the Seesaw for Schools administrators. Storage of children's work is secure and held in line with GDPR guidelines. Parents and carers are encouraged to speak to their child's teacher if they require support or have any concerns.

Security Guidelines

Backups

Files stored on the network are backed up daily. This means files can be restored if deleted or lost in error.

Save Regularly

It is important to save work regularly. If work is saved regularly and a PC or network does fail for any reason, only the work done since the last save will be lost.

Home Documents

The school cannot accept responsibility for personal documents held on school laptops; it is the responsibility of the user to back up documents created.

Offsite pupil data and pupil information

Only encrypted school laptops may be taken off site. Other school laptops and iPads must not be taken off site under any circumstances. Personal hard-drives or USB sticks used to store school work or data must be encrypted, or they must not be transported between home and school, or any other locations.

Virus Checks

All computers in school are equipped with anti-virus software. If a virus is suspected, staff members must report this immediately to a member of the senior leadership team or the computer technician.

Email Usage

Use of email and communication by email should be treated with the same degree of care that is taken when writing a letter by hand. It cannot be regarded as purely private, only to be seen by the receiver. Emails can be stored, forwarded and distributed to large numbers of people at the touch of a button. It is easy to forget that it is a permanent form of written communication and that material can be recovered even if seen to be deleted from the computer. Staff email is accessible via Outlook 2016 as a desktop app, or from within Office 365.

When using email, staff should:

- not access personal emails in school using school equipment.
- be aware that email is not a secure form of communication.
- must not forward email messages onto others unless the sender's permission is first obtained.
- must not open email attachments from unknown senders or from computers from which virus protection may not be current or activated.
- not send email messages in the heat of the moment and avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude or offensive.

Mobile devices

As a general rule, pupils are not permitted to bring mobile phones or devices into school. Should there be a need for a child to bring their device in to school, permission must be sought by the parent or carer from the school first. If it is deemed to be appropriate for a child to bring the device on to the school premises, it must be turned off and taken to the school office, where it will be stored safely. Children may collect their devices at the end of the school day. Any child bringing a mobile device onto the school premises does so at their own risk, and The Meadows Primary school cannot accept liability for devices lost or stolen when on the premises.
Mobile phones are not to be used by parents and visitors anywhere on the school site. Parents and visitors will be reminded to keep their phones out of sight when visiting the school. Staff may use their mobile phones in the staff room at break and lunch times. During the school day, mobiles should be turned off or set to silent and stored away from teaching areas. Staff must never use personal mobile devices or cameras to take images of pupils.

iPads

The school has a set of iPads which are stored centrally in the staff room, within a charging unit. Staff should complete the logbook when signing them out for class use, and once again when signing them back in. An iPad is also available for each class. Teaching staff who are assigned an iPad must ensure that the device is not left unattended. It must be kept safe when not in use. A log of iPads and their allocation details is held centrally.
Staff are required to return all devices that they have been allocated upon leaving the employment of the school.

Laptops

The school has a set of laptops which are assigned to pupils on a temporary basis for home learning. They have been formatted by the Department for Education and are equipped with antivirus and firewall software. Parents and carers are required to sign an additional acceptable use document before taking a device home (see attached).

Legal requirements

Users must agree to comply with all software license agreements. Computer facilities shall not be used to hold or process personal data except in accordance with the provisions of the Data Protection Act 2018.
Copyright Designs and Patents Act – copyright is infringed if a person acquires an unauthorised copy of a computer program. Mere acquisition, without regard to the actual or intended use, constitutes

an infringement of the author's copyright. 'Acquisition' includes loading a copy of a programme into the random access memory, or other temporary storage device, of a computer, or onto another form of permanent data storage medium.
Anyone found to have unauthorised copies of software will immediately be suspended from using IT facilities. The matter will be investigated and the necessary action taken, the school will not accept any liability.

'Hacking' is illegal under the Computer Misuse Act 1990. Regulations regarding unauthorised access or misuse of computing facilities are enforceable under the law, any person found attempting to or hacking the school network will be prosecuted.

Regulations regarding the transmission, storage or display or obscene material are enforceable by law under the Criminal Justice and Public Order Act 1984 which amends the Obscene Publications Act 1956, the Protection of Children Act 1978 and the Telecommunications Act 1984 to extend their provisions to transmission over a data communications network.

Sanctions

Failure by staff to adhere to the policy may result in the loss (temporary or permanent) of access to the school systems and may be subject to disciplinary proceedings. If the law has been broken, the police will be informed.

Managing allegations against adults who work with children and young people

Allegations made against a member of staff concerning a failure to adhere to the safe use policy should be reported to the headteacher. In the event of an allegation being made against the headteacher, the Chair of Governors should be notified immediately.

Disciplinary Procedure for all school based staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the governing body.

Additional Information

Please be aware, at such time that you leave The Meadows Primary School, your user account and any associated files, your email address and any associated emails will be removed from the school system and will no longer be accessible. The school cannot continue to receive emails sent to your email address.

Named Personnel

- Staff member responsible for E-safety and Acceptable ICT Use: Dawn Fenton (School Business Manager)
- Data Protection Officer: Wendy Gillings
- Computing and IT Subject Leaders: Andy Bell and Dan Rear
- Safeguarding Lead: Jo Simmons (Headteacher)

- Deputy Safeguarding Leads: Andy Bell (Deputy Headteacher), Karen Cassey, Nicola Richardson, Carolynn Gray

Acceptable Use Agreement for Staff, Governors and Volunteers

All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, email or social networking sites. They are asked to sign this agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I must only use the school equipment in an appropriate manner and for professional uses.
- I understand that it is my responsibility to check that children in my care have been made aware of the code of conduct for IT use before allowing them to use the network and internet in school.
- I have read the procedures for incidents or misuse in the ICT Acceptable Use Policy so that I can deal with any problems that may arise, effectively.
- I will report and document accidental misuse.
- I will report any incidents of concern for a child's safety to the headteacher (safeguarding lead) or one of nominated deputy safeguarding leads.
- I know who the nominated safeguarding leads are.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children via personal technologies, including my personal email. I know I should only use the school email address and telephones to contact parents.
- I know that I must not use the school system for personal use unless this has been agreed by the headteacher.
- I will ensure that I am familiar with and follow the Data Protection Act 2018 and General Data Protection Regulations (GDPR).
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- Should I be a member of social networking sites, I will keep my profile secure and will avoid contact with parents and pupils (including former pupils). I understand that any action or comment made by myself that brings the school or colleagues into disrepute or compromises pupil or staff confidentiality will be deemed a disciplinary matter.
- I have read, understood and agree with the Acceptable-Use policy. I know that by adhering to this, I have a better understanding of e-safety and my responsibilities to safeguard children and young people when using the school network and online technologies.

Signed: _____Date: _____

Name (printed): _____

Device loan agreement for pupils

The Meadows Primary School

1. This agreement is between:

1) The Meadows Primary School

2) Parent/Carer's name: _____

and governs the use and care of devices assigned to the parent's child (the "pupil"). This agreement covers the period from the date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

1. The school is lending the pupil laptop (Dell) for the purpose of learning at home due to school closures.

2. This agreement sets the conditions for taking a _____ school laptop home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of loan.

2. Damage/loss

By signing this agreement, I agree to take full responsibility for the loan equipment issued to the pupil and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that I and the pupil are responsible for the equipment at all times, whether on the school's property or not.

If the equipment is damaged, lost or stolen, I will immediately inform Mr. Bell and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

I will make sure my child takes the following measures to protect the device:

- Use the sleeve to protect it the laptop when transporting it from one place to another
- Keep the device in a secure place when not in use
- Don't leave the device in a car or on show at home
- Don't eat or drink around the device
- Don't lend the device to siblings or friends
- Don't leave the equipment unsupervised in unsecured areas

3. Unacceptable use

I am aware that the school monitors the pupil's activity on this device.

I agree that my child will not carry out any activity that constitutes 'unacceptable use'.

This includes, but is not limited to the following:

Include details of your acceptable use policy for devices, e.g.:

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Attempting to view age-restricted or adult content
- Using the device for social media or gaming purposes
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Causing intentional damage to ICT facilities or materials
- Using inappropriate or offensive language

I accept that the school will sanction the pupil, in line with our behaviour policy if the pupil engages in any of the above **at any time.**

4. Personal use

I agree that the pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

5. Data protection

I agree to take the following measures to keep the data on the device protected.

- I confirm that I have read the 'Getting Started' document from the Department for Education that accompanies the device
- Do not share the equipment among family or friends

If I need help doing any of the above, I will contact Mr Bell on the email office@themeadows.lincs.sch.uk

6. Return date

I will return the device, within its box, and its sleeve and charger, in its original condition to the school office within 7 days of being requested to do so.

I will ensure the return of the equipment to the school if the pupil no longer attends the school.

7. Consent

If parents are collecting the equipment, request a signed copy of this form and insert:

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

PUPIL'S FULL NAME	
PARENT'S FULL NAME	
PARENT'S SIGNATURE	