



Farmilo Primary & Nursery School

Acceptable Use Policy

Reviewed 2024

Approved on behalf of the board of governors at the meeting held on:

Date: _____

Name: _____

Signed: _____

Rationale

Learning technologies are an essential resource in Schools today and Farmilo Primary School and Nursery aims to maximise the positive impact of technology in the classroom. Technologies help to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, Schools need to build in the use of these technologies in order to arm children and young people with the skills to access life-long learning and employment.

Currently children and young people in Schools use these technologies both inside and outside of the classroom for:

- Accessing websites
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting and Streaming
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality.

Whilst these technologies are exciting and beneficial both in and out of the classroom, all Schools need to be aware of the range of risks associated with the use of these technologies.

All staff will sign and date the attached document to indicate that they have read and understood this policy and agree to comply with it.

Who this document applies to

Any member of staff or visitor, both teaching and non-teaching, who has access to the school network or Internet Connection must read, understand and sign this document prior to making use of the network/connection. Any new member of staff must be made aware of this policy and sign to confirm understanding and compliance at the earliest opportunity.

If an outside provider or visitor requires use of the school network/connection this is to be approved at the discretion of the SLT or Computing coordinator. The individual will be made aware of the general points of this policy and will be asked to sign to confirm their understanding and compliance with it.

Terms used within this document

- Appropriate: activities listed are acceptable in terms of ICT use.
- Inappropriate: activities listed as inappropriate may potentially lead to misconduct and disciplinary proceedings. In some cases this could lead to dismissal and legal action

Passwords

Access to the school server is facilitated by the school's bought-in technology service (Atom IT) and access is requested by SLT or the Computing Lead. The school is responsible for establishing and enforcing a password policy for its use of ICT. The head teacher is responsible for establishing and enforcing a password policy on their systems based on the level of security required. Passwords must be assigned to individual users of ICT systems to maintain security and the data that they contain.

Unattended machines should be left logged out or with lids closed so as to require passwords to access the server if unattended.

Appropriate:

- Users only using their own account to carry out day to day work;
- Users not disclosing their password to allow others to access their account. Users should be aware passwords are for the benefit of the school and are the proprietary and confidential information of the school;
- Users selecting a password that is easy to remember but not for others to guess;
- Users not selecting obvious passwords, such as the name of a close relative, friend or pet;
- Compliance with the password policy for each computer system.

Inappropriate:

- Requesting passwords personally assigned to other users;
- Using a session via another users password;
- Sharing passwords with other users. All users must take reasonable precautions to protect their passwords;
- If a user thinks that their username or password has been used without their permission, they must inform the head teacher as soon as practically possible. The head teacher will ensure that new users are issued with appropriate usernames and passwords. When a user leaves their job, whether leaving the school or not, the head teacher will ensure that all usernames and passwords for that user are suspended as appropriate. The head teacher may devolve responsibility for this task to the ICT coordinator or LEA Engineer at his/her discretion.
- Any inappropriate use of internet will be blocked through SECURELY and a notification sent to the Headteacher. This will be monitored in line with the Safeguarding Policy.

Use of e-mail and internet (including Social Media)

Staff only use their assigned @farmilo.notts.sch.uk e-mail address to send and receive any e-mails related to school. **Personal e-mail addresses are not used for any reasons.**

Staff should make reference to the Staff Code of Conduct for further clarification.

Whilst social media tools can provide tremendous benefits to schools they also have serious security risks in their use. In order to mitigate these security risks and still enjoy the benefits of social media schools should establish and enforce good social media usage policies which should include the following points:

- Supervision in the classroom with social media technology must be appropriate to the children's needs and abilities based on the professional judgement of the practitioner in the classroom.
- It is good practice for staff to evaluate websites before classroom use. Staff should be aware that websites, search results etc. may be safe and appropriate one day but unsafe a day later. All members of the school community should be aware that filtering software is not always effective and cannot always be relied on alone to safeguard children;
- Children with Special Educational Needs should be appropriately supported according to their specific needs and their personal understanding of the e-Safety risks;
- All pupils and staff should be aware of the school procedure regarding what to do if inappropriate content or messages are found, sent or received online. These are to be reported to the ICT Coordinator or Headteacher.

- All pupils and staff should understand how to critically evaluate online content and this is a core element of teaching in the ICT curriculum.
- Internet filtering must be in place according to the school's requirements. This should be designed with both a technical and curriculum focus and should be agreed by the schools Leadership Team and Governors;
- ICT tools provided by the school should always be used (e.g. work provided digital cameras, memory cards, laptops etc.) rather than personally owned equipment.

Use of PCs, Laptops, Servers, Technologies

Appropriate:

- Storing school data;
- Loading text, images, video or audio streams in connection with day to day work activities;
- Storing limited amounts of personal data (where agreed by the head teacher).

Inappropriate:

- Loading unauthorised or untested software;
- USB devices are not to be used without having been scanned for Viruses
- Allowing unauthorised users to access laptops used away from school;
- Failure to keep laptops used away from school secure;
- Failure to secure any device when left unattended;
- Storing confidential or personal data or information on removable media without adequate protection or encryption;
- Deliberate, reckless or negligent introduction of viruses;
- Storing personal material protected by copyright which has not been purchased;
- Loading files containing pornographic offensive or obscene material.
- Any inappropriate use of internet will be blocked through SECURELY and a notification sent to the Headteacher. This will be monitored in line with the Safeguarding Policy.

The Legal Framework

- ICT use in a school setting should be legally regulated, this includes the content of e-mail, or sites downloaded from the Internet; privacy issues, monitoring of communications and surveillance at work and employment relations. Further legal advice should be sought, if appropriate, from Council's Children and Young people's Services HR or Legal Services.
- If the school monitors e-mails or scans for profanity/inappropriate content then users should be warned of this through policies.

General Points

- Allocated passwords are kept private at all times.
- The network/connection is used only for purposes relating to the school or school life.
- Staff only use @farmilo.notts.sch.uk for e-mail related to school.
- Staff follow the practice outlined in the Safer Social Media Practice in Schools Policy
- Use of internet with children is provided with appropriate supervision.
- Best practice is to evaluate a website before directing children to use it.
- Any inappropriate content found is reported to the Headteacher or ICT coordinator. The E-Safety Policy outlines the procedure that follows this being reported.

- No unauthorised software is installed. The ICT Coordinator will liaise with the IT Engineer prior to installation of software on school technologies.
- All reasonable steps are taken to ensure the security of school technologies both on and off-site.
- A database for the use of images is held by the school and should be referred to prior to any use of pupil images.
- Copyright Laws are observed.

I have read and understood the Farmilo Primary School and Nursery Acceptable Use Policy for the use of technologies in school. I agree to comply with the policy.

[illegible]