# Moat Farm Junior School Trust
# Acceptable Use Policy (ICT) for Staff and Pupils

## 2022-2023

# Moat Farm Junior School Trust
# Acceptable Use Policy (ICT) for Staff and Pupils

**Proceeding to log on to any school equipment or the school network will be considered an agreement to the Acceptable Use Policy.**

*Having accepted this policy on the network will be considered to cover all of the valid equipment in the school. (E.g. Laptops, netbooks, desktops, tablets, etc.)* The computers, netbooks and network resources at Moat Farm Junior School, including Internet access, are available to students and staff in the school. All users are required to follow the conditions in the policy. Any breach of these conditions may lead to withdrawal of the user's access; monitoring and or retrospective investigation of the user's use of services and disciplinary action taken.

**Personal Responsibility**

Access to the computers and network resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for any damage caused, and for reporting any misuse of the computers or network to the responsible staff.

**Acceptable Use**

Users are expected to use the network systems in a responsible manner. It is impossible to set strict rules related to the use of technology at Moat Farm Junior, but the following list provides some guidelines on the matter:

1. Be polite – abusive and offensive messages will not be tolerated. You are responsible for everything you say.
2. Privacy – Do not reveal any personal information about yourself or others.
3. Password – Where applicable (i.e. All staff members), do not reveal your password to anyone. Do not share your passwords. Do not store sensitive material on class-shared user accounts.
4. E-Mail is not guaranteed to be private.
5. Disruptions – Do not use the network that would in any way disrupt the use of the network by others.
6. All staff and students should report any unsuitable websites. If a child reports material to you, report it as appropriate to the Headteacher.
7. Do not attempt to gain access to blocked material and websites. (e.g. Anonymous Proxies)

8 USB drives are not allowed in school machines.

9. Files held on the school network will be regularly checked that they are appropriate and pose no threat to the school network. Ensure that no files you are responsible for, including your user downloads and email attachments, breach this rule.
10. It is the responsibility of the user to take measures to ensure they are complying with the Acceptable Use Policy.

**UNACCEPTABLE USE**
Examples of unacceptable use include but are not limited to the following:
1. Users must log in with their **OWN** username and password where applicable and must not share this information with other users. They must also log off after their session has finished.
2. Users finding machines logged on by someone else and/or locked are not to log off or reboot the machine without permission from the person logged in.
3. Accessing, creating and transmitting offensive and inappropriate material.
4. Receiving, sending or publishing material that violates the Data Protection Act or breaching the security this law requires and copyright law.
5. Unauthorised access to data and resources on the school network or other systems.
6. User action that causes destruction or corruption of other users' data and violation of users' privacy.

**SERVICES**
There will be no warranties of any kind, expressed or implied, for the network service offered. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

**NETWORK SECURITY**
Users are expected to inform IT support or the Headteacher immediately if a security problem is identified. **Do not demonstrate this problem to other users.** Users must login with their own user id and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network.

**PHYSICAL SECURITY**
Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used. Laptops and I pads borrowed by a user not back in a locked trolley by the end of the day will be considered a breach of the Acceptable Use Policy by the user.

**WILFUL DAMAGE**
Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited. Damage to equipment in the classroom or the ICT Room will be the personal responsibility of the user. The school may monitor any activity of the user.

**Proceeding to log in will be considered an agreement to the Acceptable Use Policy.**

This policy adheres to the principles under data protection law. For further information please review the school's data protection policy published on the school's website