



Moorland Junior School

ICT AND ACCEPTABLE USE POLICY

Policy Statement

Moorland Junior School recognises that Information and Communication Technology (ICT) is an essential part of modern education. Computers, tablets, interactive screens, the internet, email, cloud platforms and other digital technologies provide valuable opportunities for learning, communication, creativity and collaboration.

The school is committed to ensuring that all technology is used:

- safely;
- responsibly;
- respectfully;
- appropriately;
- legally;
- in support of learning and school operations.

This policy establishes the expectations for the acceptable use of ICT by pupils, staff, volunteers, visitors and other users of school technology.

The policy should be read alongside the school's **Safeguarding and Child Protection Policy, Online Safety Policy, Computer Misuse and Cyber Choices Policy, Cyber Risk Assessment, Data Protection Policy, Behaviour Policy and Staff Code of Conduct.**

Scope

This policy applies to:

- school computers and laptops;
- tablets and mobile devices;
- interactive whiteboards and displays;
- school networks and Wi-Fi;
- school email accounts;
- cloud-based systems;
- learning platforms;
- school-managed applications;
- the internet;
- online communication platforms;
- removable storage devices;
- personal devices when used on school premises or for school purposes.

It applies to pupils, staff, volunteers, contractors, visitors and anyone else authorised to use school ICT.

Aims

The school aims to:

1. Provide pupils with safe access to technology.
2. Support high-quality teaching and learning.
3. Develop pupils' digital literacy and confidence.
4. Teach pupils to behave responsibly online.
5. Protect pupils and staff from inappropriate or harmful online content.
6. Protect school systems and information from cyber threats.
7. Prevent misuse of ICT.
8. Promote respect for privacy and personal information.
9. Develop pupils' understanding of their digital footprint.
10. Encourage pupils to become responsible and ethical digital citizens.

Responsibilities

The Headteacher is responsible for ensuring that:

- appropriate ICT policies and procedures are in place;
- safeguarding requirements are considered;
- staff understand their responsibilities;
- appropriate filtering and monitoring arrangements are maintained;
- serious incidents are dealt with appropriately;
- cyber security risks are regularly reviewed.

The ICT Lead or IT provider is responsible for:

- maintaining school ICT systems;
- implementing appropriate security measures;
- maintaining filtering and monitoring arrangements;
- managing user accounts and permissions;
- maintaining appropriate backups;
- applying software and security updates;
- responding to technical incidents;
- advising the school on cyber security.

Designated Safeguarding Lead

The DSL will manage safeguarding concerns arising from ICT and online activity in accordance with the school's safeguarding procedures. The DSL is responsible for oversight and review of the school's filtering and monitoring arrangements;

Staff must:

- use ICT responsibly;
- protect passwords and accounts;
- follow the school's Acceptable Use requirements;
- maintain professional boundaries;
- protect confidential information;
- report cyber security and safeguarding concerns;
- supervise pupils appropriately;
- model positive online behaviour.

Pupils are expected to:

- use technology responsibly;
- follow instructions;
- respect other people's privacy;
- keep passwords private;
- use only accounts and systems they are authorised to use;
- report anything worrying or inappropriate;
- take care of school equipment;
- follow the school's rules for internet and device use.

General Acceptable Use

Users may use school ICT for:

- teaching and learning;
- administration;
- communication;
- research;
- educational activities;
- approved enrichment activities;
- school-related creative work;
- other purposes authorised by the school.

Users must not use school ICT for activities that are unlawful, harmful, inappropriate or contrary to school policies.

Internet Use

Pupils will have access to the internet as appropriate to their age and educational needs.

The school will use appropriate **filtering and monitoring** systems to help protect pupils from harmful or inappropriate content.

Users must not deliberately attempt to access:

- pornography or sexually explicit material;
- extremist or terrorist material;
- material promoting violence or hatred;
- illegal content;
- websites designed to facilitate criminal activity;
- inappropriate gambling or age-restricted services;
- material that is inappropriate for the user's age;
- websites blocked by the school's filtering systems.

If inappropriate material appears accidentally, the user should:

1. Stop viewing it.
2. Close the page if safe to do so.
3. Tell a member of staff.

Pupils will not be punished simply because they accidentally encounter inappropriate material.

Passwords and Account Security

Users must:

- keep passwords confidential;
- use strong passwords where required;
- never share passwords with other pupils;
- never use another person's account;
- log out when required;
- lock devices when leaving them unattended;
- report suspected compromised accounts immediately.

Pupils should never attempt to guess another person's password.

Staff should use additional security measures, including multi-factor authentication (MFA), where provided by the school.

Computer Misuse

Users must not:

- access accounts without permission;
- access files they are not authorised to access;
- attempt to bypass security controls;
- attempt to bypass internet filtering;
- deliberately damage or disrupt ICT systems;
- introduce malware or harmful software;
- install unauthorised software;
- interfere with school networks;
- use hacking tools without explicit authorisation;
- deliberately delete or alter another person's work;
- attempt to gain unauthorised access to external systems.

Pupils will be taught that **being able to access something does not mean that they have permission to access it.**

Email

School email accounts should be used appropriately and for authorised purposes.

Users must:

- communicate politely;
- use appropriate language;
- check recipients before sending messages;
- take care when opening attachments;
- report suspicious emails;
- avoid sending confidential information unnecessarily;
- use school-approved accounts and platforms.

Users must not:

- send threatening or abusive messages;
- send inappropriate images;
- impersonate another person;
- deliberately send malicious messages;
- forward suspicious emails;
- share another person's personal information without permission.

Phishing and Suspicious Messages

Users should be cautious of emails or messages that:

- ask for passwords;
- request urgent financial action;
- contain unexpected attachments;
- contain suspicious links;
- claim that an account will be closed;
- appear to come from a senior member of staff but request unusual action;
- ask for confidential information.

If in doubt, users should **stop and check with a trusted member of staff or the ICT Lead**. Staff must follow the school's procedures for verifying unusual financial or sensitive requests.

Personal Data and Confidential Information

Users must protect personal and confidential information.

This includes information relating to:

- pupils;
- parents and carers;
- staff;
- safeguarding;
- medical information;
- addresses and contact details;
- school finances;
- passwords;
- staff records.

Users must not:

- share confidential information with unauthorised people;
- leave confidential information visible on unattended devices;
- upload confidential information to unauthorised services;
- use personal email accounts to send confidential school information unless specifically authorised.

Any suspected data breach must be reported immediately in accordance with the school's Data Protection Policy.

Images, Video and Audio

Images, video and audio recordings must only be made or shared for legitimate educational or school purposes, using school equipment, and in accordance with school procedures.

Users must consider:

- parental permissions where applicable;
- privacy;
- safeguarding;
- copyright;
- the dignity of pupils and staff.

Pupils must not photograph or record another pupil or member of staff without appropriate permission.

Social Media

School ICT must not be used to:

- post inappropriate or offensive material;
- bully or harass others;
- impersonate others;
- share confidential school information;
- bring the school into disrepute;
- share images of pupils without appropriate permission.

Staff must maintain appropriate professional boundaries when communicating with pupils and families online. Personal social media accounts should not be used for inappropriate communication with pupils.

Cyberbullying

Cyberbullying includes using technology to:

- threaten;
- intimidate;
- humiliate;
- embarrass;
- exclude;
- harass;
- spread rumours;
- share inappropriate images;
- impersonate another person.

Cyberbullying will be dealt with under the school's **Behaviour for Learning and Anti-Bullying Policies** and may also become a safeguarding matter.

Pupils should report cyberbullying to a trusted adult.

Mobile Phones and Personal Devices

Moorland Junior School is a mobile-free school. The use of mobile phones and personal devices by pupils will be managed in accordance with the school's separate **Mobile Phone and Personal Devices Policy**.

Unless specifically authorised, pupils must not use personal devices to:

- photograph or record others;
- access inappropriate material;
- communicate with other pupils during restricted periods;
- access school systems in an unauthorised manner;
- share confidential information.

Monitoring

Where monitoring systems identify concerning activity, the school will consider the context and respond proportionately.

Monitoring alerts may arise from:

- searches;
- websites accessed;
- keywords;
- downloads;
- attempts to access blocked material;
- unusual account activity.

An alert does not automatically mean that a pupil has deliberately done something wrong.

Reporting an ICT Incident

Users should report immediately:

- lost or stolen devices;
- suspected malware;
- suspicious emails;
- compromised passwords;
- inappropriate online content;
- cyberbullying;
- unauthorised access;
- accidental disclosure of personal information;
- attempted hacking;
- attempts to bypass filtering;
- other cyber security concerns.

Pupils should tell a trusted adult.

Staff should report incidents to the appropriate member of the school's leadership or ICT team and to the DSL where safeguarding may be involved.

Safeguarding

Online safety and ICT use form part of the school's wider safeguarding responsibilities.

The school will consider whether inappropriate ICT use may indicate:

- a safeguarding concern;
- vulnerability to online exploitation;
- harmful online influence;
- cyberbullying;
- inappropriate contact;
- exposure to harmful content;
- criminal or potentially criminal behaviour.

Safeguarding concerns will be managed in accordance with the school's Safeguarding and Child Protection Policy and current **Keeping Children Safe in Education (KCSIE)** guidance.

Consequences of Misuse

Failure to follow this policy may result in:

- removal or restriction of ICT access;
- restorative or educational work;
- behaviour sanctions;
- parental involvement;
- safeguarding intervention;
- disciplinary action for staff;
- referral to external agencies where appropriate.

Responses will be proportionate and take account of the user's age, understanding, intent and circumstances.

Acceptable Use Agreements

The school implements a range of age and role appropriate Acceptable Use Agreements.

- [EY & KS1 Acceptable Use Agreement](#)
- [KS2 Acceptable Use Agreement](#)
- [Parent & Carer Acceptable Use Agreement](#)
- [Staff & Volunteer Acceptable Use Agreement](#)
- [Staff Use of AI Acceptable Agreement](#)

Review

This policy will be reviewed annually or sooner where required by:

- changes in technology;
- changes to legislation or safeguarding guidance;
- significant cyber or online safety incidents;
- changes to school systems;
- changes to filtering or monitoring arrangements.

REVIEWED AND UPDATED	SIGNED ON BEHALF OF THE SCHOOL	DATE FOR REVIEW
August 2026	Ashleigh Brotherton	August 2027