Emmaville Primary School

ICT and Internet Acceptable Use Policy

2023-2025

Date	Review Date	IT Coordinators	Nominated Governor
October 2023	October 2025	Sue Lawrence Kit Saddington	Bill Purvis

Contents

---

1. Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

> Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors

> Establish clear expectations for the way all members of the school community engage with each other online

> Support the school's policy on data protection, online safety and safeguarding

> Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems

> Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our Choices Policy (Management of Behaviour Policy)/ staff code of conduct.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

> Data Protection Act 2018

> The General Data Protection Regulation

> Computer Misuse Act 1990

> Human Rights Act 1998

> The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

> Education Act 2011

> Freedom of Information Act 2000

> The Education and Inspections Act 2006

> Keeping Children Safe in Education 2020

> Searching, screening and confiscation: advice for schools

3. Definitions

> **"ICT facilities"**: includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service

> **"Users"**: anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors

> **"Personal use"**: any use or activity not directly related to the users' employment, study or purpose

> **"Authorised personnel"**: employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities

> **"Materials"**: files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

> Using the school's ICT facilities to breach intellectual property rights or copyright

> Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination

> Breaching the school's policies or procedures

> Any illegal conduct, or statements which are deemed to be advocating illegal activity

> Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

> Activity which defames or disparages the school, or risks bringing the school into disrepute

> Sharing confidential information about the school, its pupils, or other members of the school community

> Connecting any device to the school's ICT network without approval from authorised personnel

> Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data

> Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel

> Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities

> Causing intentional damage to ICT facilities

> Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel

> Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation

> Using inappropriate or offensive language

> Promoting a private business, unless that business is directly related to the school

> Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher or ICT Coordinator will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion. Discussion, acceptance and written agreement must be first obtained.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's Choices Policy (Management of Behaviour Policy) / staff code of conduct.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's IT Service Provider, Omnicom Solutions, manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

> Computers, tablets and other devices

> Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT Coordinator or Omnicom, or speak in person with Omnicom Technical Support at the time of the scheduled fortnightly visit.

5.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils, and should not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the ICT Coordinator and/or the Headteacher immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff should use phones provided by the school to conduct all work-related business whenever possible. (N.B. In the event of staff working from home – during Covid-19 isolation, for example – the caller ID display function on their phone must be deactivated before any work-related calls are made to parents.)

School phones must not be used for personal matters.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

> Does not take place during contact time/teaching hours.

> Does not constitute 'unacceptable use', as defined in section 4

> Takes place when no pupils are present

> Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's mobile phone device policy.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely. This is provided through RD Web Access, using their RemoteApp and Desktop Connection service. The service is managed by Omnicom Solutions as part of the school's service package, and is accessed via personalised username and password authentication.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. The school's network offers the same security and protection remotely, as it does while being used in the school itself, but staff must still take such precautions as the Headteacher or ICT Coordinator may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy, which can be found on the GDPR section of the school's website.

5.4 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

> Internet sites visited

> Email accounts

> Telephone calls

> User activity/access logs

> Any other electronic communications

The school uses Securus software (provided by Omnicom Solutions) to monitor all PC, laptop and tablet use in the school. This software constantly scans and monitors keyboard and screen use for incidences of unacceptable use, taking screen captures that are stored for up to 45 days. Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

> Obtain information related to school business

> Investigate compliance with school policies, procedures and standards

> Ensure effective school and ICT operation

> Conduct training or quality control exercises

6. Pupils

6.1 Access to ICT facilities

Use of laptops and iPads are available pupils for educational purposes only under the supervision of staff. See the school's Computing Policy for the ICT use in the curriculum. This policy can be found on the Computing Page in the Curriculum section of the school's website.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the Choices Policy (Management of Behaviour Policy), if a pupil engages in any of the following **at any time** (even if they are not on school premises):

> Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination

- Breaching the school's policies or procedures

- Any illegal conduct, or statements which are deemed to be advocating illegal activity

- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

- Activity which defames or disparages the school, or risks bringing the school into disrepute

- Sharing confidential information about the school, other pupils, or other members of the school community

- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel

- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities

- Causing intentional damage to ICT facilities or materials

- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation

- Using inappropriate or offensive language

We ask pupils in Year 3 and 4 and their parents/carers to read and sign the agreement in appendix 3, and those in Year 5 and 6 to read and sign appendix 2.

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to sign the agreement in appendix 1.

8. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy, which can be found in the GDPR section of the school's website.

8.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices. These access rights are managed by the ICT Coordinator via Omnicom Solutions.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the ICT Coordinator immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by Omnicom.

9. Internet access

The school wireless internet connection is secured. Anti-viral software is installed on all machines that connect to the internet, including firewall and filtering, provided and managed by Omnicom.

If any inappropriate websites are accessed by staff or children that the filter has not successfully identified, staff must report this immediately to the ICT Coordinator or Omnicom.

9.1 Pupils

Pupils have access to the school's wifi only in terms of their use of school laptops or iPads to use the internet for education purposes. Pupils do not have access to the school's wifi for their own personal use or for use on their own devices. Details of the wifi address and password is not available to pupils.

9.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

> Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)

> Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10. Monitoring and review

The headteacher and ICT Coordinator monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every 2 years.

The governing board is responsible for approving this policy.

11. Related policies

This policy should be read alongside the school's policies on:

- E-safety Policy
- Safeguarding Policy
- Choices Policy (Management of Behaviour Policy)
- Staff Code of Conduct
- Data protection Policy
- Privacy Notice
- Data Breach Policy
- Remote learning Policy

Acceptable use of the internet: agreement for parents and carers
Name of parent/carer: **Name of child:**
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Our school website – for information about the school and its curriculum, including diary dates, policies and current newsletters. • Email/text groups for parents (via ParentMail – for reminders, newsletters & announcements) • SeeSaw – for children/parents to post homework/comments & for teachers to respond to these • Marvellous Me – for teachers to send short administrative messages/reminders/information to parents, as well as to send documents, photos of children's work and 'badges' informing them of notable achievements in the classroom etc.   Parents/carers may choose to set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure   I will not: • Use private groups or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way • Use private groups or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers
Signed:	**Date:**

Appendix 2: Acceptable use agreement for older pupils

<table>
<tr><td colspan="2" align="center">Acceptable use of the school's ICT facilities and internet:
agreement for KS2 pupils</td></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">

When using the school's ICT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break school rules
- Access any inappropriate websites
- Make internet searches using inappropriate language or images
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password (for apps I use in school or at home) with others or log in using someone else's details
- Bully other people

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems, including any internet searches I make, or any words or phrases I type into a device.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
</table>

Acceptable use of the school's ICT facilities and internet: agreement for younger pupils

Name of pupil:

When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails, or when I type on any device
- Share my passwords (for apps I use in school or at home) at school with others or log in using someone else's name or password
- Bully other people

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	Date:

Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors
Name of staff member/governor/volunteer/visitor:
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**