

# Lockington CE VC Primary School



## ICT and internet acceptable use policy

Date Policy Formally Agreed By Governors:	20 <sup>th</sup> April 2023
Date Policy Becomes Effective:	20 <sup>th</sup> April 2023
Review Date:	Summer term 2024
Person Responsible for Implementation and Monitoring:	Headteacher & Administration Officer

## 1. Introduction and aims

Information and communications technology (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, and the pastoral and administrative functions of the school. However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding. In order to keep the school community safe whilst working online and using ICT we have developed this policy.

This policy also needs to be read in conjunction with the following policies: Strategic Safeguarding and Child Protection, Computing, Behaviour and Discipline & Data Protection as well as the East Riding of Yorkshire Council policies and guidance for the Use of the Internet and Use of Electronic Mail.

The policy reflects the school's aims and values and sets out what the school considers 'Acceptable Use' of ICT resources for all users of our computer network. It sets out a framework in which teaching and non-teaching staff can operate.

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 policies on data protection, online safety and safeguarding
- Prevent disruption that could occur 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.

## 2. Relevant legislation and guidance

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

- [Data Protection Act 2018](#)
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- [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](#)
- [Education and Inspections Act 2006](#)
- [Keeping Children Safe in Education 2022](#)
- [Searching, screening and confiscation: advice for schools 2022](#)
- [National Cyber Security Centre \(NCSC\): Cyber Security for Schools](#)

- [Education and Training \(Welfare of Children\) Act 2021](#)
- [UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- [Meeting digital and technology standards in schools and colleges](#)

### 3. Definitions

- **ICT facilities:** 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 school's ICT service
- **Users:** anyone authorised by the school to use the school's 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 agreed by an authorised user
- **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 school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 6 for a glossary of cyber security terminology.

### 4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct (as per the staff code of conduct) the matter will be dealt with in accordance with staff disciplinary procedures. The action taken will depend upon the individual circumstances, nature and seriousness of the specific incident.

Unacceptable use of the school's ICT facilities includes:

- To breach intellectual property rights or copyright
- 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
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- 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 programme, tool or item of software designed to interfere with the functioning of the school's 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 the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel 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 or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

#### **Exceptions from unacceptable use**

Where the use of school ICT facilities (on the school premises and/or remotely) 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.

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

##### **Access to school ICT facilities and materials**

The administration officer, headteacher and IT Provider (SMD) manage access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files
- Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.
- Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the administration officer or headteacher.

Staff should sign the agreement in appendix 4.

##### **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 must 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. Emails sent by staff should not contain children's names and instead make use of initials.

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 that contains the personal information of another person, they must inform the data protection officer (SLA) via the headteacher immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents or pupils. School phones must not be used for personal matters unless authorised by the headteacher.

### **Personal use**

Staff are permitted to use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The headteacher may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching time
- 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 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 use of social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

### **Personal social media accounts**

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times. Staff are responsible for any content they post and should not publish content relating to Lockington CE VC Primary School or East Riding of Yorkshire Council.

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

### **Remote access**

We allow staff to access school's ICT facilities and materials remotely with the permission of the Headteacher.

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. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the network manager and Headteacher may require 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.

### **School social media accounts**

The school has an official Facebook and Twitter account, managed by the administration officer. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

### **Monitoring and filtering of the school network and use of ICT facilities**

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of: internet sites visited, bandwidth usage, email accounts, telephone calls, user activity/access logs and any other electronic communications. Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The effectiveness of any filtering and monitoring will be regularly reviewed. Where appropriate, authorised personnel may raise concerns about monitored activity with the school's designated safeguarding lead (DSL) and ICT manager, as appropriate.

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, prevent or detect crime, comply with a subject access request, Freedom of Information Act request, or any other legal obligation. The governing board will regularly review the effectiveness of the school's monitoring and filtering systems.

## **6. Pupils**

### **Access to ICT facilities**

Pupils have access to laptops, iPads and ICT equipment only under the supervision of staff. Children are not permitted to use school equipment for personal use. They are not permitted to use personal ICT equipment in school. Children who do not have an Acceptable Internet Use Statement (Appendix 3) agreed on their behalf by their parent/carer will not be allowed to use the internet. This means they will therefore not be able to access all statutory content of the computing curriculum.

## **7. Parents**

### **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.

### **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 adhere to the statement (Appendix 2).

## **8. Data security**

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on [digital and technology standards in schools and colleges](#), including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

### **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.

### **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 have these installed, and 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.

### **Data protection**

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

### **Access to facilities and materials**

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

## **9. Protection from cyber attacks**

Please see the glossary (appendix 6) to help you understand cyber security terminology.

The school will:

- Work with governors, SMD and Schools' IT to make sure cyber security is given the time and resources it needs to make the school secure
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks
- Put controls in place that are: proportionate, multi-layered, up to date & regularly reviewed and tested
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to Schools' IT and SMD.
- Have a firewall in place that is switched on
- Work with our LA and SMD to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

## **10. Internet access**

The school's wireless internet connection is secure. However, filters are not fool proof and any issue with the filtering system should be reported to Schools IT or SMD via the administration officer or headteacher.

Parents and visitors to the school will not be permitted to use the school's Wi-Fi 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 Wi-Fi 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 Wi-Fi password to anyone who is not authorised to have it.

## **12. Related policies**

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

- E-safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Remote education





## 11. Monitoring and review

The headteacher, administration officer and computing governor monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed annually.

The governing board is responsible for approving this policy.

Signed:  Headteacher Date: 20<sup>th</sup> April 2023

Signed:  Chair of Governors Date: 20<sup>th</sup> April 2023

## Appendix 1: Facebook cheat sheet for staff

**Do not accept friend requests from pupils on social media**

### 10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if you don't, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or pupils)

---

### Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to [bit.ly/2MdQXMN](https://bit.ly/2MdQXMN) to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to [bit.ly/2zMdVht](https://bit.ly/2zMdVht) to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

### What to do if ...

### **A pupil adds you on social media**

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

### **A parent adds you on social media**

- It is at your discretion whether to respond. Bear in mind that:
  - Responding to 1 parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
  - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

### **You're being harassed on social media, or somebody is spreading something offensive about you**

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

## Appendix 2: Acceptable use of the internet: statement for parents and carers

### Acceptable use of the internet: statement for parents and carers

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Our official Facebook and Twitter accounts
- Email/text groups for parents
- Our website

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, the school's Facebook page, 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 unless they are raised in an appropriate way
- Use private groups, the school's Facebook page, 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 the other children's parents/carers

### Appendix 3: Acceptable use agreement for pupils

#### Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

**When I use the school's ICT facilities (like computers and equipment) and go 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
- Go on Facebook or other social networking sites (unless as part of a lesson)
- 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
- Share my password 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:

**Parent/carer agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

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
- 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:**

## Appendix 5: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) [glossary](#).

TERM	DEFINITION
<b>Antivirus</b>	Software designed to detect, stop and remove malicious software and viruses.
<b>Breach</b>	When your data, systems or networks are accessed or changed in a non-authorized way.
<b>Cloud</b>	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
<b>Cyber attack</b>	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
<b>Cyber incident</b>	Where the security of your system or service has been breached.
<b>Cyber security</b>	The protection of your devices, services and networks (and the information they contain) from theft or damage.
<b>Download attack</b>	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
<b>Firewall</b>	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
<b>Hacker</b>	Someone with some computer skills who uses them to break into computers, systems and networks.
<b>Malware</b>	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
<b>Patching</b>	Updating firmware or software to improve security and/or enhance functionality.
<b>Pentest</b>	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
<b>Pharming</b>	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.

TERM	DEFINITION
<b>Phishing</b>	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
<b>Ransomware</b>	Malicious software that stops you from using your data or systems until you make a payment.
<b>Social engineering</b>	Manipulating people into giving information or carrying out specific actions that an attacker can use.
<b>Spear-phishing</b>	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
<b>Trojan</b>	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
<b>Two-factor/multi-factor authentication</b>	Using 2 or more different components to verify a user's identity.
<b>Virus</b>	Programmes designed to self-replicate and infect legitimate software programs or systems.
<b>Virtual private network (VPN)</b>	An encrypted network which allows remote users to connect securely.
<b>Whaling</b>	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.