Acceptable Usage Policy

Lionel Walden Primary School

Updated:

November 2023

Review Date:

November 2024

Contents

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 (including the senior leadership team), 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.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers 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.

Breaches of this policy may be dealt with under our behaviour policy for children and out code of conduct policy and disciplinary policy for adults.

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 2023
- 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
- UK Council for Internet Safety (et al.) 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 that 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. 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
- 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 and other senior leaders 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.

4.1 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. All incidents of this type must be approved by the headteacher or senior leaders before commencement

Where the use of AI tools such as ChatGPT are used, these must only be used as a research tool to help find out about new topics and ideas. AI-generated must be properly attributed and not be passed off as the users own work.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school’s policies on disciplinary, behaviour and code of conduct.

The school reserves the right to revoke privileges to the use of the school systems should it deem appropriate and proportionate.

The school will deal with any infringements by children as a learning opportunity for all and will respond in a manner that is both constructive and reflective. It is not our desire to withhold ICT from pupils as this invariably is counterproductive, however procedures may be put in place to limit what, where, when and how children can access digital ICT hardware and software.

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

5.1 Access to school ICT facilities and materials

Then ICT Service ultimately manages access to the school's ICT facilities and materials for school staff. The headteacher and other senior members of staff have the facility to manage some access to the school ICT facilities. This 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 headteacher or other their line manager.

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. Staff should ensure that access to their email account remains secure at all times. If accessing emails via phone, staff must ensure that their phone is suitably protected from unauthorised access eg by passcode, finger print or face recognition.

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/carers and pupils with the intention of using these for the purpose of communicating regarding school related activities, 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.

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 headteacher or a senior member of staff immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the school to conduct all work-related business. In the event that a personal mobile phone is required to contact a parent/carer, then the holder must withhold their number by using 141 before dialling.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

Staff who would like to record a phone conversation should speak with the headteacher. All recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

Request for recording phone conversations will be agreed on a case by case basis. Examples of the types of requests for recording are as follows:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents/carers to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.
- Discussing requests for term-time holidays

5.2 Personal use

Staff are permitted to occasionally 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 contact time and 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 personal electronic smart device policy (mobile phone 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/carers 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.

5.2.1 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.

Members of staff should ensure that they employ appropriate security settings for social media accounts such as Facebook and Instagram. The school has guidelines for staff on appropriate security settings for certain social media accounts such as Facebook(see appendix 1).

5.3 Remote access

The school uses a Windows 365 tenancy, which means that staff are able to gain access to files and documents outside of the school network via Microsoft OneDrive.

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. Access to the Microsoft 365 suite of programs including

OneDrive must be protected by suitable means such as passwords. If staff access these services on machines other than school laptops, all relevant safety precautions must be employed. Staff must ensure that they sign out fully to protect files and documents from unauthorised access. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and must take such precautions as 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.

5.4 School social media accounts

The school has an official Facebook account, managed by the headteacher and other staff designated by the headteacher. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the administration areas of the account.

The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

5.5 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
- 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 school's internet connection is supplied by EastNet and is filtered and monitored by Smoothwall.

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

Our governing board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place. The school uses Smoothwall to filter and monitor online activity
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns

    - Smoothwall provide weekly updates to senior leaders to inform them of any inappropriate activity by users online.

- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and headteacher, as appropriate.

6. Pupils

6.1 Access to ICT facilities

The following ICT facilities are available to pupils attending the school:

- Computers and iPads are available to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Pupils will be provided with an account linked to the school's network and Microsoft 365 environment, which they can access from any device

6.2 Search and deletion

Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the headteacher, can search pupils and confiscate their mobile phones, computers, cameras or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- An item that is identified as inappropriate to be brought to school and could potentially cause distress or harm to self or others, **and/or**
- Can access the internet by utilising means other than the schools secure network connection, **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from a senior leader or a member of the safeguarding team
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation. If the pupil refrains from cooperating, then senior leaders and safeguarding personnel must be called. At this point, parent/carers may be called.
- The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of an item that could breach this policy or impact safeguarding
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL, headteacher and other senior leaders to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the 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 breach intellectual property rights or copyright
- 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 making 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
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- 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 the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

Please refer to section 4.2 above on Sanctions.

7. Parents/carers

7.1 Access to ICT facilities and materials

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

However, parents/carers 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/carers 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/carers 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/carers to abide by the principles set out in appendix 2.

7.3 Communicating with parents/carers about pupil activity

The school uses online facilities such as identified websites eg BBC Online and National Geographic as part of general usage. The school also uses search engines to allow children to research and find relevant information for a particular purpose.

Occasionally, we may inform parents and carers to make them aware of any online activity that their children are being asked to carry out if it differs greatly from normal classroom practice. This may mean that we provide you with specifics before the children, so that you can prepare for any questions that may arise from it. This might include visiting particular websites or searching for particular content.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

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/carers 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

8.1 Passwords

All users of the school's ICT facilities are set 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, visitors or volunteers who disclose account or password information may have their access rights revoked.

It may be necessary to update password periodically to ensure safety of accounts. Users will be notified when passwords require changing or a change has taken place.

We encourage the setting of strong passwords.

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 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.

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.

Our data protection policy can be found on our 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 Service.

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 headteacher or ICT Service 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 shut down completely at the end of each working day.

8.5 Encryption

The school makes sure 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 the ICT Service.

9. Protection from cyber attacks

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

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
  - Check the sender address in an email
  - Respond to a request for bank details, personal information or login details
  - Verify requests for payments or changes to information
- 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, as this would not guarantee recovery of data
- Put controls in place that are:
  - **Proportionate**: the school will verify this using a third-party audit (such as 360 degree safe) at least annually, to objectively test that what it has in place is effective
  - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
  - **Up to date:** with a system in place to monitor when the school needs to update its software
  - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data from the schools server daily and store these backups on cloud-based backup systems that are not connected to the school network and which can be stored off the school premises
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to IT Provider – The ICT Service
- Make sure staff:
  - Enable multi-factor authentication where they can, on things like school email accounts
  - Store passwords securely
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on

- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with our local authority 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 and password protected. It is monitored by the ICT Service. The connection contains appropriate filtering via Smoothwall that blocks content based on staff or pupil log in details. Whilst this is effective, no system is 100%. If staff are alerted to any sites that are deemed inappropriate the should:

- If the material is on a child operated device, then either remove device or turn of the screen.
- If possible, note the address of the inappropriate site
- Alert the headteacher or a senior leader immediately with details of the site
- The headteacher or a senior leader will inform the ICT Service to deal appropriately with any infringements

10.1 Pupils

Pupils will only be able to access the internet via the schools WiFi connection. Pupils will:

- Be taught how to search effectively and safely for information
- Will learn how to identify results and pages that are deemed inappropriate
- Will know how to report anything online that they feel uncomfortable with or deem inappropriate or offensive
- Will understand that our WiFi is filtered and monitored at all times and that they use it in a respectful and correct way

10.2 Parents/carers and visitors

Parents/carers 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/carers 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.

11. Monitoring and review

The headteacher and governors 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 every 2 years or sooner if government policy or safeguarding aspects change.

The governing board is responsible for reviewing this policy.

12. Related policies

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

- Online safety
- Social media
- Safeguarding and child protection
- Behaviour
- Staff Code of Conduct
- Staff discipline
- Data protection
- Mobile phone or smart device usage

Appendix 1: Guidance for using social media when working in education

Lionel Walden Primary School recognizes that access to technology in school gives students, parents and teachers greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st-century technology and communication skills.

To that end, this Acceptable Use Policy outlines the guidelines and behaviors that users are expected to follow when using school technologies.

Students, parents and teachers are expected to follow the same rules for good behavior and respectful conduct online as offline.

Misuse of social media can result in disciplinary action.

We work hard to ensure childrens' safety and security online, but cannot not be held accountable for any harm or damages that result from misuse of social media technologies outside of the school.

We encourage teachers, students, staff, and other school community members to use social networking/media (Twitter (X), Facebook, WhatsApp etc.) as a way to connect with others, share educational resources, create and curate educational content, and enhance the classroom experience. While social networking is fun and valuable, there are some risks you should keep in mind when using these tools. In the social media world, the lines are blurred between what is public or private, personal or professional.

We've created these social networking/media guidelines for you to follow when representing the school in the virtual world.

Please do the following:

- We expect you to use good judgment in all situations.
- You must know and follow the school's Code of Conduct and Privacy Policy.
- Regardless of your privacy settings, assume that all of the information you have shared on your social network is public information.
- Do not engage or talk about situations that arise in school that identify individuals
- Always treat others in a respectful, positive and considerate manner and act in a way that does not bring the school into disrepute
- Report any online activity that you think is inappropriate to your line manager or the headteacher. You may also follow the school's Whistleblowing Policy

Don't share the following:

- Do not engage or talk about situations that arise in school that identify any individuals
- Do not publish, post or release information that is considered confidential or not public. If it seems confidential, it probably is. Online "conversations" are never private
- Do not post pictures of colleagues without their permission
- Do not post pictures of children from the school without the expressed consent of their parents

Be cautious with respect to:

- the type and amount of personal information you provide. Avoid talking about personal schedules or situations.
- The types of things that you post online. Remember that current and future employers have a duty to check out a person’s social media presence and act accordingly should anything untoward be found.
- Who you befriend online. It is generally not acceptable to be friends with children from the school. Communicating with children online can sometimes lead to difficulties with safeguarding and is very much discouraged.

If allegations are made against any member of staff, please note that the school will act according to the policy for Safeguarding and Child Protection, the Code of Conduct for staff and the Whistleblowing Policy.

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

Acceptable use of the internet to communicate with or about the school
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following online channels: • Our official Facebook page • The school's website page • Evidence Me (Pre School & Reception only) • Email
When communicating with the school via official communication channels, or using private/independent channels to talk about the school: • 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 The use of private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff is not a constructive way to express views and the school can't improve or address issues unless they are raised in an appropriate way The 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 is not constructive way to solve issues. Contact the school and speak to the appropriate member of staff if you are aware of a specific behaviour issue or incident. Uploading or sharing photos or videos on social media of any child other than my own is strongly discouraged, unless you 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

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 my teacher said I could as part of a lesson)
- 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
- Send any photos, videos or livestreams of people (including me) who aren’t wearing all of their clothes
- Use the camera facility to take inappropriate pictures and store them on the device or network
- 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 impose sanctions if I do certain unacceptable things online, even if I’m not in school when I do them.

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

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 any private business, 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.

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
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	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
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	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.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.