ICT Acceptable Usage Policy

Policy Version Control	
Policy type	Trust
Policy prepared by (name and designation)	Chris Carr – Head of IT
Last Review Date	November 2025
Description of changes	Full policy review to adopt recommendations from Veritau our DPO and also to recognise the in house IT provision
Date of Trustee Approval	27th November 2025
Date released	27th November 2025
Next review date	Autumn 2028

1. Introduction

1.1 The Lingfield Education Trust embraces modern and emerging technologies that enhance teaching, learning, and operational efficiency. As digital tools evolve rapidly, our Trust is committed to using them safely, responsibly, and effectively to benefit all learners and staff.

> "Digital technologies provide powerful opportunities for collaboration, creativity, and learning. To use them effectively requires awareness of both the benefits and risks, and a commitment to safe, ethical, and informed practice."
> — Department for Education, Digital and Technology Standards, 2023

2. Scope

2.1 This policy applies to all users of Trust owned or Trust managed digital systems, including staff (of any contract term), students, volunteers, contractors, agency workers, visitors, and anyone granted access to Trust technology or data ("Users").

2.2 This policy covers all sites, devices, systems, and services managed by or on behalf of the Lingfield Education Trust, including cloud services, network infrastructure, and remote access. Individual schools may append additional guidelines to meet local operational needs, provided these align with this overarching policy.

3. Purpose

3.1 The purpose of this policy is to:

- Safeguard and protect children, staff, and all digital users within the Trust community.
- Support the safe and responsible adoption of new and emerging technologies that enhance learning and teaching.
- Ensure all users understand their professional, ethical, and legal obligations regarding digital conduct, security, and data protection.
- Promote a culture of digital responsibility, respect, and resilience.

4. General Guidelines for All Users

4.1 Security and Privacy

- Users must never share their passwords or login credentials with others. Passwords must be strong, unique, and comply with the Trust's security policy.
- All Trust systems use Multi-Factor Authentication (MFA) where available; users must ensure MFA is enabled and configured correctly.
- Attempts to bypass or disable security controls (e.g., firewalls, filtering, endpoint management) are strictly prohibited.
- Users must immediately report suspected data breaches, account compromises, or phishing attempts.
- The use of removable media (USB drives, Portable Hard drives) is discouraged. When necessary, only Trust-issued, encrypted media may be used, and only for temporary data transfer in compliance with the Trust's Data Protection procedures.
- All Trust data must be stored in approved, secure locations. These are typically within Microsoft 365, or other approved cloud systems.

4.2 Equipment and Hardware Use

- All Trust hardware and devices remain the property of the Trust and must be used responsibly, professionally, and in accordance with Trust policy.
- Devices must be secured when unattended and stored safely when not in use.
- Food and drink must not be consumed near IT equipment.
- Personal use of Trust devices should be limited and must not interfere with professional duties or compromise security.
- Devices must not be loaned to family, friends, or unauthorised users.
- All Trust devices are subject to management, monitoring, and security compliance checks.
- Users must not install unauthorised software, applications, or extensions, nor alter system configurations (e.g., jailbreaking, rooting, or unauthorised modification).

4.3 Faults, Loss, or Damage

- Faults, damage, or loss must be reported immediately to the Trust IT department.
- Theft, deliberate damage, or negligence may result in disciplinary action and possible personal liability for repair or replacement.
- Devices lost or stolen off-site must be reported to the Trust IT Service Desk and, if applicable, to the police.

5. Communication and Internet Use

5.1 Professional Communication

- Staff must use their official Trust or school-provided email accounts for all work-related communication.
- Personal email accounts must never be used to send or receive work-related data.
- Digital communications should be professional, respectful, and compliant with the Trust's Safeguarding and Behaviour policies.
- Inappropriate, discriminatory, or offensive communication whether internal or external is strictly prohibited.
- Users must not send confidential or sensitive information through unsecured channels (e.g., unencrypted email). Approved secure methods such as encrypted file sharing or M365-protected messages must be used.

5.2 Online Conduct and Safety

- Users must not access, upload, download, or share any material that is illegal, discriminatory, abusive, or inappropriate for an educational setting.
- Any accidental access to such material must be reported immediately to the Headteacher or designated safeguarding lead.
- Users must remain alert to phishing, scams, and social engineering attempts and must complete regular cybersecurity awareness training provided by the Trust.
- The use of social media or online platforms in a professional capacity must comply with the Trust's Social Media Guidance within the Code of Conduct Policy

6. Data Protection and Information Governance

- All users must comply with the **UK GDPR**, **Data Protection Act 2018**, and the Trust's Data Protection and Information Security policies.
- Sensitive or confidential data (such as personal, safeguarding, or pupils' sensitive information) must only be shared where strictly necessary and using approved secure methods.
- Before sharing data with third parties, staff must confirm that a valid Data Sharing Agreement or contract is in place.
- Only the minimum necessary data should be shared, and personal identifiers should be redacted whenever possible.
- If users are uncertain about whether data is considered sensitive or confidential, they must seek advice from the Trusts DPO Veritau.

7. Remote Access, Hybrid Working, and Microsoft Teams Data

- Remote access to Trust systems (including Microsoft 365, Teams, SharePoint, and other approved cloud services) is granted on a case-by-case basis and may be withdrawn at any time. Access is managed in line with the Trust's cybersecurity and safeguarding requirements.
- When working remotely, users must ensure they are in a secure environment and connected to a private, trusted network. Public Wi-Fi networks should be avoided where possible.
- All devices used to access Trust systems remotely must be enrolled in the Trust's device management system (such as Microsoft Intune) to ensure compliance with encryption, anti-malware, and security-update standards, and to enable remote lock or wipe if required.
- All remote sessions, logins, and data activity are automatically logged through Microsoft 365 conditional access and security auditing tools. These logs may be reviewed for safeguarding, compliance, or cybersecurity purposes.
- Users must only access, create, and store Trust data through approved Microsoft 365 applications (e.g., Teams, SharePoint, and OneDrive for Business). Files shared or created in Teams channels are automatically stored within the associated SharePoint site and must not be downloaded or copied to personal or unmanaged storage.
- The use of third-party VPNs, remote desktop tools, file transfer services, or unapproved cloud platforms (e.g., personal Google Drive, Dropbox,

or iCloud) to access or store Trust data is strictly prohibited.

- Sensitive or confidential data must never be downloaded from Microsoft Teams or SharePoint to personal devices or shared outside of approved Teams channels or Trust groups without explicit authorisation.

- Users are personally responsible for ensuring that any data accessed or worked on remotely remains within the secure Microsoft 365 environment at all times.

8. Cloud Services and Collaboration Tools

- The Trust supports the use of cloud-based platforms (e.g., Microsoft 365) that comply with UK GDPR and DfE digital standards.

- Data owners (schools, departments, or teams) retain responsibility for how their information is stored and shared.

- Users must manage access permissions carefully, ensuring that data is only visible to authorised users.

- Sensitive or personal data should only be stored in approved systems with encryption and access control.

9. Artificial Intelligence (AI) and Emerging Technologies

The Trust only accepts responsible use of AI tools by Staff to enhance learning, creativity, and efficiency when the following principles are adhered to.

- Users must not input personal, confidential, or sensitive information into AI tools or platforms unless explicitly approved and compliant with data protection requirements.
- Users must ensure that AI technologies accessed comply with UK GDPR regulations

- Staff must apply professional judgement when using AI-generated content, ensuring accuracy, fairness, and ethical integrity.

- All users must comply with the Trust's AI policy

10. Breaches of Policy

Any breach of this policy, whether intentional or accidental, may result in disciplinary action up to and including dismissal. In serious cases, breaches may also result in referral to external authorities or regulatory bodies.

11. Legal and Regulatory Framework

All users must comply with relevant UK legislation, including but not limited to:

- Data Protection Act 2018 and UK GDPR
- Computer Misuse Act 1990
- Communications Act 2003
- Copyright, Designs and Patents Act 1988
- Malicious Communications Act 1988
- Protection of Children Act 1978
- Sexual Offences Act 2003
- Equality Act 2010
- Online Safety Act 2023

12. Definitions

Confidential / Sensitive Information: Any information that could identify individuals, compromise privacy, or cause harm to the Trust, pupils, or staff if disclosed.

Remote Access: Secure connection to Trust systems or data from a non Trust location.

Cloud Services: Secure, internet-hosted platforms approved by the Trust for storage, communication, and collaboration. These include Arbor and other cloud related services.

AI Tools: Software or services that use artificial intelligence or machine learning to generate or process information.

Appendix One – Workforce Acceptable Use

The document governs our workforce's use of the trust network and cloud-based systems, including when authorised to use personal devices.

Email, Instant Messaging, and Internet Use

We provide our staff with email accounts, instant messaging and (IM) functionality (TEAMS), and Internet access to assist with performing their duties.

Personal use
Whilst email accounts, IM, and the Internet should primarily be used for business functions, incidental and occasional use in a personal capacity may be permitted so long as users understand the following:

- Use must not tarnish our reputation or infringe on business functions
- Emails sent to and from trust or school accounts are our property

- We may monitor the use of accounts and systems and access any personal messages and browsing history contained within
- Emails sent to or from their email account may be disclosed under Freedom of Information and/or Data Protection Legislation
- We reserve the right to cleanse email accounts at regular intervals, which could result in personal emails being erased from the corporate network
- We reserve the right to suspend access to accounts and systems anytime.

Inappropriate use
We do not permit users to send, forward, or solicit emails, or use the Internet in any way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit or pornographic messages, images, cartoons, jokes, or movie files
- Unwelcome propositions, profanity, obscenity, slander, or libel
- Any messages or content containing ethnic, religious, political, or racial slurs
- Any messages or content that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Users are also not permitted to use the Internet in a way that could affect others' usage. This means not streaming or downloading media files and not using the Internet to play online games.

Other business use
Users are not permitted to use emails or the Internet to carry out their own business or the business of others. This includes, but is not limited to, work for political organisations, not-for-profit organisations, and private enterprises. The SIRO may lift this restriction on a case-by-case basis.

Security
Users will only use corporate accounts and systems in accordance with our Information Security Policy. In particular, users will not:

- Click on links from untrusted or unverified sources
- Use insecure email transmission methods when sending personal data
- Sign up for marketing material that could jeopardise our IT network
- Send excessively large email attachments without prior authorisation from the SIRO and/or our IT Provider
- Attempt to download any software onto corporate devices. This can present a virus risk and/or breach of software license requirements.

Group email accounts
Users may be permitted to send and receive emails from group and/or generic email accounts. These group email accounts must not be used in a personal capacity, and users must ensure that they sign each email with their name so that emails can be traced to individuals. Improper use of group email accounts could lead to the suspension of a user's email rights.

The SPOC will be responsible for allowing access to group email accounts. All email traffic to and from individual and group accounts may be monitored.

Social Media and Private Messaging Apps

We recognise and embrace the benefits and opportunities that social media can contribute to a school. However, we also recognise that social media poses a data protection risk due to its open nature and capacity to broadcast to many people quickly.

Trust or School accounts
We may have social media accounts across multiple platforms. Nominated users will have access to these accounts and are permitted to post general information about our business activities. Authorised users will be given the usernames and passwords to these accounts, which must not be disclosed to any other user within or external to the organisation. The SPOC will be responsible for allowing access to school social media accounts.

School social media accounts must not be used to disseminate personal data in an open forum or by direct message. Doing so would be a contravention of our information governance policies and data protection legislation.

Trust or School accounts must not be used in a way which could:

- Tarnish our reputation
- Be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs
- Be construed as sexually explicit
- Be construed as political beliefs or commentary.

Personal accounts
We understand that many users will use or have access to personal social media accounts. Users must not use these accounts:

- During working hours
- Using trust equipment
- To conduct school or trust business
- To contact or approach our clients, customers, or partners
- Make posts that relate to us or refer to information gained through your role within the organisation
- Identify your role within our organisation.

Private messaging apps
Information held on messaging apps such as WhatsAPP, Facebook Messenger in non-corporate communication channels may be subject to FOIA if it relates to official business. Therefore we advise caution is applied if this platform is ever used for such purposes, and should only be done so when other communication methods are unavailable

Telephone and Video Conferencing Use

We provide users access to telephone and video conferencing services to assist with communication and performing their duties.

Personal use
Whilst telephone and video conferencing services should primarily be used for education functions, incidental and occasional use in a personal capacity may be permitted so long as users understand the following:

- Usage must not tarnish our reputation or infringe on business functions
- We may monitor and access call history and recordings
- We reserve the right to suspend telephone and video conferencing usage at any time
- Telephone calls, video conference recordings, or transcripts may be disclosed under the Freedom of Information and/or Data Protection Legislation.

Inappropriate use
We do not permit users to use the telephone or video conferencing services in any way which may be interpreted as insulting, disruptive, or offensive by any other individual or entity.

Other business use
Users are not permitted to use these services to carry out their own business or the business of others. This includes work for political organisations, not-for-profit organisations, and private enterprises. The SIRO may lift this restriction on a case-by-case basis.

Appendix Two - Pupil Acceptable Use - Primary

Information for Parents and Guardians

Digital technologies have become integral to children's and young people's lives, both within and outside school. These technologies are powerful tools that open up new opportunities for everyone. They can stimulate discussion, promote creativity, and raise awareness, which promotes effective learning. Young people should always be entitled to safe digital and Internet access.

This Acceptable Use Agreement is intended to ensure that:

- pupils will be responsible users and stay safe while using the Internet and other digital technologies for educational, personal and recreational use
- our digital systems are protected from accidental or deliberate misuse that could put the security of our systems and users at risk
- parents and guardians are aware of the importance of e-safety and are involved in the education and guidance of young people regarding online behaviour.

Pupil Acceptable Use Agreement

I understand that I must use digital technology responsibly by doing the following:

- I will only use computers or tablets with permission from a teacher or a suitable adult.
- I will only use applications that a teacher or a suitable adult has allowed me to use.
- I will take care of the computer, tablet, and other equipment.
- I will ask for help from a teacher or a suitable adult if I am unsure what to do or think I have done something wrong.
- I will tell a teacher or a suitable adult if I see something that upsets me on the screen.

I have read and understand the above and agree to follow these rules when:

- I use the school systems and devices (both in and out of school).
- I use my own equipment outside of school in a way related to schoolwork, e.g. communicating with other pupils or teachers, accessing school email, website, etc.

If I break the rules, I might not be allowed to use a computer or tablet for schoolwork.

Pupil name:
Class:
Pupil signature:
Date:

Parent or Guardian Permission

As the parent or guardian of the named pupil, I give permission for my child to access the Internet and digital systems at school.

I know that my child has signed this Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the Internet, both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that my child is safe when using the Internet and digital systems.

I understand that my child's activity on digital systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to use the Internet and digital technologies safely at home and will inform the school if I have concerns about my child's e-safety.

Parent or guardian name:
Parent or guardian signature:
Date: