ICT Acceptable Usage Policy

Policy Version Control				
Policy type		Multi Academy Trust		
Policy prepared by (name and designation)		Tristen Coad		
Document Owner		Data Protection Officer		
Date of Governing Body approval		6 October 2022		
Date released		6 October 2022		
Version	Changes	Author	Date of Issue	Date for Review
1.0	• Document creation	T. Coad (DPO)	02/07/2021	08/07/2022
2.0	• Annual Review • Policy Type Amendment	T. Coad (DPO)	12/09/2022	12/09/2023
2.1	• Amendment to section 5.3 • Creation of new section 5.4 relating to data transferring	T. Coad (DPO)	03/10/2022	12/09/2023

1. Introduction

1.1 The Lingfield Education Trust embraces any new and emerging technologies where educational benefits are seen to be available. There are many new digital resources being made available each and every day.

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners. To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

2. Scope

2.1 This document has been written in order to produce clear guidelines for everyone in each school, including but not limited to staff (any-term), volunteers, agency staff, visitors, students and any other users of Information Communication Technology (ICT) at the Academy Trust. Hereinafter referred to as "Users".

2.2 This policy applies to all sites in the trust however, where applicable, the individual sites may append additional guidelines to this policy based on a specific individual need or requirement.

3. Purpose

3.1 The main purpose of this document is as follows:

• To safeguard and protect the children and users within schools and wider trust community,

• To safely embrace any new and emerging technologies if deemed to be of benefit to pedagogical practices within the trust including but not limited to teaching and learning.

• To assist users working with children in the safe and responsible use of ICT and web-based services,

• To ensure that all members of the trust and school communities are aware of their professional and legal obligations in regards to ICT responsibilities and expectations while working for The Lingfield Education Trust.

4. General Guidelines for all Parties

4.1 Security and Privacy

4.1.1 Users of trust or school ICT hardware, infrastructure or services must not disclose any password, login name given or security detail, to anyone, or allow anyone else to use their account. Re-use of "standard" passwords is also not permitted, passwords must be unique across services and accounts. Users must also ensure that passwords are sufficiently strong, in compliance with any and all security policies for the trust.

4.1.2 No attempt to circumvent the security or protection of the trust or school network or any trust or school device is permitted.

4.1.3 The trust strongly discourages the use of removable media however if they are used to store any sensitive information The Trust will only allow the use of hardware-based encrypted USB media with a minimum of Real-time military grade XTS-AES 256-bit Hardware Encryption and crypto-parameters protected with SHA-256 hashing. This encrypted media is to be used solely for a means of transportation outside the locality of the school or trust office in any way e.g. sent off-site electronically or by post or courier.

4.2 Equipment / Hardware, Safe and Responsible use thereof

4.2.1 The consumption of food or drink is strictly prohibited whilst using trust or school hardware. It is hazardous to the equipment and to individuals.

4.2.2 Sensible, responsible and appropriate use of any trust or school hardware is expected at all times.

4.2.3 Under no circumstances should trust or school hardware be loaned for any term, to non-school or trust users. This includes but is not limited to user's friends, family or others.

4.2.4 Any device provided for your use, shall at all times remain the property of the trust or school. The trust or school reserves the right to require the return of its portable devices at any time.

4.3 Faults, Loss or Damage

4.3.1 Any faults should be reported promptly to the schools technical support provider at the earliest opportunity. Loss of, or damage to the portable device should also be reported immediately to the schools technical support provider. In the case of theft, wilful damage or serious neglect you may personally be liable for the cost of the device/s in question.

4.4 Tampering and unapproved modification of devices

4.4.1 Under no circumstances should the operating system or installed applications on any trust or school provided devices be modified by the user in any way, this includes

but is not limited to "Hacks", "Mods", "Jailbreaks", or any other actions that may interfere with the originally indented operation of the device.

5. Internet and E-Mail usage

5.1 Staff are not permitted to use "personal" e-mail accounts for any work-related purpose. Personal e-mail access is permitted, however this must be for personal use only. All official communications should be carried out using the official school or trust e-mail provided.

5.2 Use of e-mail and communication by e-mail should be treated with the same degree and care you would take if you were to write a letter to the person that you are contacting by email. It cannot be regarded as purely private, only to be seen by the receiver. E-mail can be stored, forwarded and distributed to large numbers of people at the touch of a button. It is easy to forget that it is a permanent form of written communication and that material can be recovered even if seen to be deleted from the computer.

5.3 When using e-mail, users should:

• Be aware that e-mail is not a secure form of communication and therefore no personal information should be sent,

• Not forward e-mail messages onto others unless the sender's permission is first obtained. Especially in cases where the communication is outside of the organisation.

• Not use email communication to forward business sensitive, commercially sensitive and/or confidential documentation to actors outside of the organisation.

• Must not open e-mail attachments from unknown senders,

• Must not send e-mail messages in the heat of the moment and avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude or offensive

5.4 Lingfield Education Trust stores a large volume of business sensitive, commercially sensitive and confidential data, which may need to be shared in specified instances, e.g. children's data shared with NHS services, etc. All members of staff must read, understand and adhere to the Trust's separate GDPR Policies concerning data and information security.

Sensitive data, for the purpose of this document, includes data which contains:

- Business and commercially sensitive data concerning the Trust and its Academies;
- Confidential data about the Trust, its Academies, ~~its~~ staff and pupils;
- Confidential data about the Trust's goods, services and products;
- Sensitive data relating to Trust partners and suppliers

If anyone handling data is any doubt as to whether that data is or is not 'sensitive data', they must refer the matter to their line manager.

Data (sensitive or not) should only be transferred where it is strictly necessary for the effective running of the Trust and/or its Academies. Before any data transfers are requested, the necessity of the transfer should be considered in advance.

When dealing with third parties consider whether any data sharing agreements or contracts are in place that cover the transfer of that data. Check whether there are any stipulations in place regarding the method of transfer that should be used.

Check that you are not providing more information than is necessary for the identified purpose. For example, do not just send a whole document or spreadsheet when only one section or specific columns are required.

For all transfers of information containing personal or sensitive data, it is essential that you appropriately establish the identity and authorisation of the recipient.

Before choosing the method of transfer, you must consider the following:

- The nature of the information, its sensitivity, confidentiality or possible value
- The size of the data being transferred
- The damage or distress that may be caused to individuals as a result of any loss during transfer
- The implications any loss would have for the school
- You must only send information that is necessary for the stated purpose, and any data not required should be redacted or removed completely (as appropriate) before transfer.

5.5 The guidance in this policy will apply to any electronic communication, including but not limited to e-mail, web services, chat rooms, forums, bulletin and news group or peer to peer sharing etc.

5.6 Please remember that the school email system is owned by the trust and any mail arriving at this email system is the electronic property of the trust. The email system may be monitored and interrogated.

5.7 Inappropriate material

5.6.1 Under no circumstances should users view, upload or download any material that is likely to be unsuitable for children or users at each school or trust. This applies to any material of violent, dangerous, racist, or inappropriate sexual content. If users are unsure about this, or any materials, users must ask their line managers or the schools technical support provider.

If in doubt, do not use. The transmission, storage, promotion or display of offensive, defamatory or harassing material is strictly forbidden as they breach the laws of the UK under the Computer Misuse Act. Possession of certain types of unsuitable material can lead to personal prosecution by the police.

5.6.2 Any unsuitable or inappropriate materials found on a school or trust network or the Internet, by accident or otherwise, must be reported immediately to the Executive Head Teacher/Head Teacher/Deputy Head Teacher/School Business Manager/Technical Support Provider (or as appropriate). Details must include the location and nature of the material including the Internet addresses (URLs) where applicable to allow removal or filtering to be applied, or for disciplinary action to be taken if appropriate.

6. Copyright and Licencing

6.1 Users accessing software or any services available through a school must be in compliance with any licence agreement and/or contract terms and conditions relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.

6.2 Do not download, use or upload any material that is subject to third-party copyright. Always seek permission from the owner before using any material from the Internet. If in doubt, or you cannot obtain permission, do not use the material.

7. Guidelines for Staff - remote access to school or trust systems (VPN)

7.1 Where approved, remote access enables you to work on files and potentially have access to SIMS / The MIS and other school systems and data from off-site. This increases the risk of other people gaining access to important and confidential information and means that staff need to be particularly vigilant when leaving their device unattended if using Remote Access. The Information Commissioner's Office (ICO) has judged both schools and individuals very harshly when lax procedures and practice have resulted in data protection breaches.

7.2 Remote access is provided to any user on a case-by-case basis. Requests for access should be made by a user's line manager; requests may be refused and previously approved access may be revoked without justification.

7.3 VPN usage must adhere to all existing trust policies and comply with all public legal frameworks including, but not limited to all relevant Data Protection legislation and regulatory requirements.

7.4 All users hereby agree that VPN usage data (Connection times, IP address', file access etc) is recorded and subject to audit.

7.5 VPN usage potentially leverages a user's personal / home internet connection. Therefore connection quality may vary and additional service charges may apply, dependent on a user's service plan subscription.

7.6 The Lingfield Education Trust Remote Access System is the only Trust approved method to access Trust systems from a remote location with the exception of email access via the web login portal. VPN software and connections from other providers are strictly forbidden and no attempt to setup VPN software and connection on personal devices to Trust systems should be made. This item does not include remote desktop technologies used by third-party support providers to support Trust systems via contracted services.

7.7 With the VPN connection active, all communications traffic will be directed through the trust or school network and will be subject to controls, policies and network/firewall restrictions.

8. Use of cloud-based storage and services

8.1 The trust does not endorse the use of one particular cloud-based solution over any other. However any chosen system must have completed the Department for Education self-certification checklist (details of which can be found here: https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act). The Trust do insist that any system used is done so in a managed, informed and legal way. Including adherence to the following guidelines.

8.2 Managed use – At all times the individual data controlling entity retains full responsibility for how the data they control is used and accessed. Therefore a method of securing and managing access to the data, including audit functions and potential revocation of any user's access to the data, is essential and must be ensured by the controlling entity.

8.3 The transfer of any data to any cloud service does not transfer liability or responsibility away from the controlling entity. Any and all legal frameworks are still applicable in regards to data protection and use of the data.

8.4 The trust strongly recommends that no sensitive or personal data be transferred, for any term, to any cloud service. Usage should be limited to collaborative working and strategic data rather than any sensitive or personal information.

9. Breaches of policy

9.1 Any violation of the standards, procedures or guidelines set out in this policy may be treated as a formal trust disciplinary matter, which could result in dismissal, legal prosecution or both.

10. Legal frameworks

10.1 It is the users responsibility to ensure they are compliant and work within all UK and E.U. applicable legislation in regards to the safe and legal use of ICT at the school or trust, this includes but is not limited to the following:

• The Sexual Offences Act 2003
• The Racial and Religious Hatred Act 2006
• The Computer Misuse Act 1990 (sections 1 – 3).
• The Police and Justice Act 2006
• Communications Act 2003
• Data Protection Act 2018
• The General Data Protection Regulation (GDPR)
• Malicious Communications Act 1988
• Copyright, Design and Patents Act 1988
• Public Order Act 1986
• Protection of Children Act 1978
• Obscene Publications Act 1959 and 1964
• Protection from Harassment Act 1997.
• The Regulation of Investigatory Powers Act 2000 (RIP)
• The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

11. Definition of terms

"Confidential" or "sensitive" information includes, but is not limited to:

• Person-identifiable information, e.g. student and employee records protected by the Data Protection Act 1998,

• Information divulged with the expectation of confidentiality,

• Academy, Trust or Council business or corporate records containing organisationally or publicly sensitive information,

• Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and politically sensitive information.

"Remote access" - Non-local access to any academy/Trust system/s or services,

"VPN" – Virtual private networking. Technical terminology for "remote access",

"Licence" - An agreement between two parties for use of a specific system or service,

"Upload" - The act of publishing any data on the internet or cloud service, in any way perceived public or private,

"Download" - The act of copying or removing data from the internet or cloud service

"Mobile use" - Use of any hardware while mobile in any way.