LDST
Liverpool Diocesan Schools Trust

ICT Regulations

Contents Page

1. Introduction

1.1. The Liverpool Diocesan Schools Trust (the Trust) has a statutory duty to keep children safe whilst receiving education through its schools. This is set out in the government's guidance 'Keeping Children Safe in Education' (KCSiE[1]).

1.2. This duty extends to both on-site and remote learning. These ICT regulations therefore set out the minimum standards required of the Trust's ICT environment to enable safe learning in line with KCSiE whether on school sites or through remote provision.

1.3. This document is approved annually by the Board of Directors and applies to the Trust, all its Schools and, if applicable, its subsidiary undertakings.

1.4. Compliance with these regulations is compulsory for all staff connected with the Trust and its Schools. A member of staff who fails to comply with these Regulations may be subject to disciplinary action under the Trust's disciplinary policy and the Board of Directors will be notified of any such breach. It is the responsibility of individual school Senior Leadership Teams (SLT) and Local Governing Bodies (LGB) to ensure that staff are made aware of the existence and content of the Trust's ICT Regulations.

1.5. In exceptional circumstances, the Board of Directors may authorise a departure from the detailed provisions of these regulations. In such circumstances, the Chief Operating Officer will maintain an appropriately detailed dispensation register to formally record such decisions.

1.6. These regulations should be read in conjunction with other relevant Trust policies, in particular the Data Protection Policy, Freedom of Information Policy, Remote Learning Policy, Acceptable Use Policies and Artificial Intelligence Policy.

2. Organisational Roles and Responsibilities

2.1. The responsibility for keeping children safe in education extends to all employees and Directors of the Trust. The following, however, sets out the specific aspects of those responsibilities relating to the ICT control environment.

2.2. **The Board of Directors** of LDST are responsible for

2.2.1. Approving a set of ICT regulations which meet the statutory duties set out in government guidance and regulation; and

2.2.2. Monitoring Trust-wide compliance with the defined ICT regulations.

2.3. **The Chief Operating Officer (COO)** is responsible for:

2.3.1. Establishing a set of ICT regulations which meet the statutory duties set out in government guidance and regulation;

2.3.2. Obtaining assurance around the compliance with the defined regulations and reporting routinely to the Board of Directors.

2.4. **The Data Protection Officer (DPO)** is responsible for:

[1] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

2.4.1. Informing and advising the Trust and its employees of their obligations under the General Data Protection Regulations (GDPR) and other data protection related legislation;

2.4.2. Monitoring compliance with the Trust's data protection related policies; and

2.4.3. Providing advice in relation to Data Protection Impact Assessments.

2.5. **Local Governing Bodies** are responsible for:

2.5.1. Receiving assurance that all school staff and visitors are made aware of the existence and content of the Trust ICT regulations;

2.5.2. Monitoring compliance with the defined ICT regulations for their school;

2.5.3. Providing assurance to the Board of Directors via the Chief Operating Officer around the school's approach to meeting the requirements of and ensuring compliance with the ICT regulations.

2.6. **Headteachers** are responsible for:

2.6.1. Communicating the existence and content of the ICT regulations to all staff, and visitors, and providing assurance to the LGB that this is the case;

2.6.2. Identifying and addressing any instances of non-compliance;

2.6.3. Providing the LGB, COO or Board of Directors with necessary data or information to provide assurance over the systems of control implemented and the compliance with those controls.

2.7. **The Trust IT Service Provider** is responsible for advising the Chief Operating Officer and the Board of Directors on the regulations and technical aspects required to meet the statutory duties set out in government guidance.

2.8. **Schools IT Service Providers** are responsible for implementing measures as instructed by schools to meet the requirements set out in these regulations.

2.9. **Internal auditors** will be engaged by the Board of Directors to routinely monitor compliance with regulations and provide recommendations to improve and/or strengthen the overall ICT control environment. The internal auditors will provide independent and objective assurance on the adequacy and effectiveness of design and implementation of the systems of internal control.

2.10. **Other roles and responsibilities**. Should any other specific role or responsibility with respect to the ICT control environment not be clearly defined above, the Chief Operating Officer should be consulted to determine the most appropriate group to perform the role.

3. ICT Controls

3.1. Appropriate Access

3.1.1. A fundamental requirement underpinning these ICT regulations is that users of the ICT systems are individually identifiable, and that activity undertaken by each individual can be tracked. It is therefore essential that each individual users' access to systems is appropriately secured.

3.1.2. Shared accounts should be avoided. Where several users require access to a single mailbox for instance, this can be achieved through shared access from individual accounts rather than a shared account. Any instances of shared accounts must be reported to and authorised by the Chief Operating Officer,

and wherever possible be replaced with shared access through individual accounts as soon as practicable.

3.1.3. The Trust must be assured that schools' ICT systems include appropriate security arrangements to prevent unauthorised access to individual accounts. Specifically, systems should include as a minimum:

- Strong password requirements (i.e. a sufficiently long and complex combination of letters, numbers and special characters); and
- Two-factor authentication for access when not connected directly to a Trust or school-controlled network.

3.2. Appropriate Filtering

3.2.1. The Trust is required to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering[2].

3.2.2. The Trust is expected to assess the risk of our children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology.

3.2.3. The Trust is obliged to ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the schools' IT systems.

3.2.4. However, schools need to be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

3.2.5. The Trust must be assured that schools' systems ensure that access to illegal content is blocked, specifically that filtering providers:

- are Internet Watch Foundation (IWF) members and block access to illegal Child Sexual Abuse Material (CSAM); and
- integrate the 'police assessed list of unlawful terrorist content, produced on behalf of the Home Office'.

3.2.6. Recognising that no filter can guarantee to be 100% effective, the Trust must be assured that schools' filtering systems manage the following content:

- Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of protected characteristics listed in the Equality Act 2010.
- Drugs / Substance abuse: displays or promotes the illegal use of drugs or substances.
- Extremism: promotes terrorism and terrorist ideologies, violence or intolerance.
- Malware / Hacking: promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content.
- Pornography: displays sexual acts or explicit images.

[2] https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-for-england-and-wales

- Piracy and copyright theft: includes illegal provision of copyrighted material.
- Self Harm: promotes or displays deliberate self harm (including suicide and eating disorders).
- Violence: displays or promotes the use of physical force intended to hurt or kill.

3.2.7. The above list should not be considered exhaustive.

3.2.8. The Trust must be assured that schools' filtering systems meets the following principles:

- Age appropriate / differentiated filtering: includes the ability to vary filtering strength appropriate to age and role.
- Circumvention: the ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services, and DNS over HTTPS.
- Control: the ability and ease of use that allows schools to control the filter to permit or deny any specific content.
- Filtering Policy: a published rationale that details the approach to filtering with classification and categorisation as well as over blocking.
- Group / Multi-site Management: the ability to deploy central policy and obtain central oversight.
- Identification: the system can identify specific users.
- Mobile and App content: the system is effective in blocking inappropriate content via mobile and app technologies.
- Multiple Language Support: the ability for the system to manage relevant languages.
- Network Level: wherever possible, filtering is applied at the network level rather than being reliant on software on user devices.
- Reporting Mechanism: the ability to report inappropriate content for access or blocking.
- Reports: the system offers clear historical information on the websites visited by users and the preventative measure taken where applicable (i.e. sites blocked).

3.3. Appropriate Monitoring

3.3.1. The Trust must be assured that appropriate monitoring systems are in place commensurate to the learning environment and the level of risk. This will include a combination of:

- physical monitoring: physical supervision of children while using the internet or monitoring of screen activity through other technological means whilst physically in the same location;
- internet and web access monitoring: review of log files or reports to identify trends in online activity and intervene with issues concerning access or searches; and

- active/proactive technology monitoring services: technology-based monitoring systems that actively monitor usage through keywords and other indicators across devices. Such systems may also provide live monitoring of activity.

3.3.2. Recognising that no monitoring can guarantee to be 100% effective, the Trust must be assured that schools' monitoring systems at least covers the following content:

- Illegal: content that is illegal, for example child abuse images and terrorist content.
- Bullying: involve the repeated use of force, threat or coercion to abuse, intimidate or aggressively dominate others.
- Child Sexual Exploitation: is encouraging the child into a coercive or manipulative sexual relationship. This may include encouragement to meet.
- Discrimination: promotes the unjust or prejudicial treatment of people on the grounds of protected characteristics listed in the Equality Act 2010.
- Drugs / Substance abuse: displays or promotes the illegal use of drugs or substances.
- Extremism: promotes terrorism and terrorist ideologies, violence or intolerance.
- Pornography: displays sexual acts or explicit images.
- Self Harm: promotes or displays deliberate self harm.
- Violence: displays or promotes the use of physical force intended to hurt or kill.
- Suicide: suggests the user is considering suicide.

3.3.3. The Trust must be assured that schools' monitoring systems meet the following principles:

- Age Appropriate: includes the ability to implement variable monitoring appropriate to age. This will in turn define which alerts are prioritised and responded to.
- Data Retention: complies with existing Trust data retention policies.
- Devices: only devices capable of implementing the monitoring system are used.
- Flexibility: changes in monitoring policy (e.g. addition or removal of keywords) can be undertaken easily and quickly.
- Group / Multi-site Management: the ability to deploy central policy and obtain central oversight.
- Impact: the ability to track the impact of monitoring activity.
- Monitoring Policy: Users are aware that their online activity is being monitored and why.
- Multiple Language Support: the ability for the system to manage relevant languages.

- Prioritisation: Alerts generated via monitoring are prioritised to enable a rapid response to immediate issues.
- Reporting: Alerts are recorded, communicated, and escalated appropriately.

3.4. Minimum Standards and Specific Requirements

3.4.1. All schools must be compliant with the minimum standards required to achieve the National Cyber Security Centre (NCSC) 'Cyber Essentials'[3] certification.

3.4.2. All schools must be compliant with or working towards achievement of the digital and technology standards in schools and colleges as set by the Department for Education[4].

3.4.3. All school staff are required to have an LDST email account (firstname.surname@ldst.org.uk or firstinitial.surname@ldst.org.uk) which is used to access LDST resources including email and intranet.

3.4.4. All correspondence relating to school or Trust activity must be conducted using LDST email accounts. Where schools have a legacy email account associated with their local authority or under a separate domain, these must be forwarded to the equivalent LDST account and ultimately closed down within a 6-month period of transfer into the Trust.

3.4.5. Artificial Intelligence (AI) technologies introduce a range of potential risks, including data protection breaches, unreliable or misleading outputs, bias, and the inadvertent disclosure of confidential or personal information. Accordingly, users are required to exercise professional judgement and must not submit sensitive data to AI systems unless expressly permitted. All AI use must align with the Trust's AI Policy, which sets out detailed expectations for safe, ethical, and compliant use.

[3] https://www.ncsc.gov.uk/cyberessentials/overview

[4] https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges

Appendix A – Baseline Security Checklist

The following list is a baseline security checklist to support schools and their IT providers to meet the ICT regulations:

- ☐ All school infrastructure is protected with secure, complex passwords. These are changed on a regular basis, and the top-level 'full access' accounts are only used when required.
- ☐ The default passwords for all devices are changed before they are allowed onto the network.
- ☐ Security updates are applied to all network devices on a monthly basis. Only devices that are compatible with the latest Operating Systems and security patches are allowed on the network.
- ☐ Unmanaged and unsecured devices are not allowed onto the school network.
- ☐ School staff are not provided with the wireless network password for the secure network. Instead, an isolated guest (BYOD) network is provided for this function.
- ☐ Staff have restricted access to the network that grants them the most limited set of permissions needed for their role, reducing the risk of a security breach by preventing accidental contamination.
- ☐ Spam filtering is applied to the school email system to reduce the likelihood of phishing emails being received by the end user and protections are in place to prevent someone from impersonating a school user.
- ☐ Our network does not allow users to download or access any installation files that could compromise the network.
- ☐ Only the IT team can install and manage software. This prevents users from downloading software that appears legitimate but can track usage and slow down the network.
- ☐ Staff are not granted local administrator permissions except in exceptional circumstances.
- ☐ A remote access solution is available that allows staff to work on files from home. Users are not permitted to download files or transfer any files onto the network. The remote access solution only authorises connection to a specific part of the network.
- ☐ An up-to-date anti-virus and ransomware protection system is in place.
- ☐ An up-to-date firewall system is in place.
- ☐ Users have access to the most up-to-date version of Microsoft software.
- ☐ School servers and critical workstations are updated with the latest patches on a termly basis to reduce the potential for issues that could affect performance and reliability. Exceptions to this are limited and made only when required.
- ☐ Network infrastructure devices have their firmware updated on an annual basis, or as required in the event of a critical update / compatibility issue arising.
- ☐ Data is backed up each night to a storage array. Physical and logical access to this is restricted to protect the files from attack.
- ☐ Critical data is backed up to the cloud.

- ☐ All network devices are audited every 12 months and a full security review carried out for each device. Any that do not meet the new standards are removed from the network.
- ☐ Staff laptops are encrypted using BitLocker technology before being allowed off site.
- ☐ Office 365 Rights Management Protection is used to provide a secure and encrypted e-mail facility.
- ☐ Staff receive regular training on the correct usage of the school system.
- ☐ Staff are aware that they can, and feel confident to, speak with the IT team if they are unsure of anything.
- ☐ Staff receive advice and information via e-mail during periods of high cyber-security threat.
- ☐ Staff are given advice and guidance on the proper use of the school network to reduce the risk of contamination.
- ☐ Staff are supported with the correct use of their home computers, and where possible are assisted to ensure they make informed and secure decisions to reduce the risk to the school's/Trust's network.
- ☐ Disclaimers are automatically added to incoming mail to continually remind users of the risk from phishing e-mails.

Appendix B - Review and Revision Schedule

Review Schedule

Policy Author	Chief Operating Officer (COO)
Policy Approver	Board of Directors
Current Policy Version	1.4
Policy Effective From	July 2026
Policy Review Date	By July 2028

Revision Schedule

Version	Revisions	By whom
1.0	Original document produced	TCSD
1.1	Updates reflecting recommendations from audit reports, updated guidance from central government, and minor changes to terminology and job titles.	TCSD
1.2	Minor updates for typographical errors and updating the Trust prayer.	TCSD
1.3	Minor updates.	TCSD
1.4	Additional context related to AI and other minor updates	COO