Lancaster School
Part of the SEN Trust Southend

POLICY

Access Control Policy

Dominic Wan
ICT Officer

Table of Contents

1 Introduction

Lancaster School (LS) implements physical and logical access controls across its networks, IT systems and services in order to provide authorised, auditable and appropriate user access ensuring appropriate data confidentiality, integrity and availability.

Access control systems are in place to protect the interests of all authorised users of LS IT systems by providing a safe, secure and accessible environment in which to work.

1.1 Scope

This policy covers all LS networks, comms room, IT systems, data and authorised users.

1.2 Out of Scope

This policy does not cover LS external website and other information classified as 'Public'.

Systems outside LS control will not fall under Sections 2.2.1 and 2.2.2.

Access to non-LS resources and applications is the responsibility of the system, resource or application owner. The Authorisation and auditing processes involved in granting access to these resources is the responsibility of the resource owners.

2 Policy

2.1 Principles

LS will provide all employees, students, volunteers and contracted third parties with on-site access to the information they need to carry out their responsibilities in as effective and efficient manner as possible.

LS will also provide off-site access to third parties in accordance with Section 2.2.1.4.

2.1.1 Generic Identities

Generic or group IDs shall not normally be permitted as means of access to LS data, but may be granted for unusual circumstances if sufficient controls on access are in place.

Existing generic IDs in current effect are accounts for Cottage guests, lunch club, holiday club and visitors to the school. All have very restrictive privileges.

Generic IDs will never be used to access confidential data or personally identifiable data.

2.1.2 Privileged accounts

The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted, controlled and not provided by default.

Authorisation for privilege accounts should not be granted lightly. IT should guard against issuing privilege rights to entire teams to prevent potential losses of confidentiality and / or integrity (such as malicious attacks which can use the privileges to control a machine).

2.1.3 Least Privilege and need to know

Access rights will be accorded following the principles of least privilege and need to know. Need to know limits information access to the information that an individual requires to carried out their responsibilities. Least privilege extends this concept to system privileges.

2.1.4 Maintain data security levels

Every user should understand the sensitivity of their data and treat it accordingly. Even if technical security mechanisms fail or are absent, every user should attempt to maintain the security of data appropriate to its sensitivity.

Users electing to place information on non-LS managed systems and databases, digital media, cloud storage or removable storage devices are advised only do so if protective measures (such as the use on encryption) is implemented. Users are consequently responsible that appropriate access to the data is maintained.

User are obligated to report instances of non-compliance to LS via the school office.

2.2 Access Control Authorisation

2.2.1 User accounts

Access to LS IT resources and services will be given through the provision of a unique user account and password.

2.2.1.1 Staff User Accounts

Staff user accounts are provided when a member of staff starts their employment.

By default curriculum staff will have access (in addition to their own personal drive) to the teacher drive, student work drive, media drives and archive. Access to further drives will depend on the teams they work with. Teaching staff will also be provided with a LS email address. All staff will have access to a standard suite of software.

By Default administration staff will have access to the winpool drive and sims drive.

Upon termination of contract, staff user accounts will be disabled for 1 year and then deleted.

2.2.1.2 Student User Accounts

Student user accounts are provided when they start.

By default students will have access (in addition to their own personal drive) to the student work drive, media drives and archive.

Upon leaving the school, student accounts will be disabled for 1 year and then deleted.

2.2.1.3 Guest Account

Guests and visitors to the school can have access to a guest account which will permit them temporary access to the internet and the basic software suite. The guest account cannot access any data drive.

2.2.1.4 Third Parties

Third parties should not be provided access unless there is exceptional circumstances. If access is provided is should adhere to Section 2.1.3. If no longer required or at the end of contract the accounts should be removed.

Unless needed, third party accounts will be disabled when not in use. Request for use should be sent via email stating name of technician, purpose of work and duration. All third party access will be logged.

2.2.2 Passwords

Student passwords (due to the needs of the students) will follow a uniformed pattern.

Staff passwords must meet length and complexity requirements which are controlled via Active Directory. They must be a minimum of eight characters, both types of case and at least either a digit or symbol.

Teacher iPad passwords must be a minimum of 6 digits, iPad's used by students are not password protected, but have restricted internet use.

Passwords can be changed via the IT Support Desk.

Comment [DW1]: Just need to check whit Tom how we are going to proceed with this section.

2.2.3 Access Permissions Matrix

All users have different permissions depending on what their job role is. Staff members who also are part of a team may have different permissions in addition to their job role permissions.

All access permissions adhere to Section 2.1.3.

2.2.3.1 Office Domain Network Drives

Postholder	Admin	Management	Personnel	Sims	Winpool	Work Experience
SBC Support	**Full Control**	**Full Control**	**Full Control**	**Full Control**	**Full Control**	**Full Control**
Administrative Staff	No Access	No Access	No Access	**Read, Write & Modify**	**Read, Write & Modify**	No Access
Management Team	No Access	**Read, Write & Modify**	No Access	**Read, Write & Modify**	**Read, Write & Modify**	No Access
Work Experience	No Access	No Access	No Access	No Access	No Access	**Read, Write & Modify**
Teachers	No Access	No Access	No Access	No Access	No Access	No Access
LSAs	No Access	No Access	No Access	No Access	No Access	No Access
Students	No Access	No Access	No Access	No Access	No Access	No Access
Visitor	No Access	No Access	No Access	No Access	No Access	No Access

2.2.3.2 Curriculum Domain Network Drives

Postholder	Admin	Archive	Photos	Student Work	Teachers	Videos	Pastoral
SBC Support	**Full Control**	**Full Control**	**Full Control**	**Full Control**	**Full Control**	**Full Control**	**Full Control**
Administrative Staff	No Access	**Read**	**Read, Write & Modify**	No Access	**Read, Write & Modify**	**Read, Write & Modify**	No Access
Management Team	No Access	**Read**	**Read, Write & Modify**	No Access	**Read, Write & Modify**	**Read, Write & Modify**	No Access
Work Experience	No Access	No Access	No Access	No Access	No Access	No Access	No Access
Teachers	No Access	**Read**	**Read, Write & Modify**	**Read, Write & Modify**	**Read, Write & Modify**	**Read, Write & Modify**	No Access
LSAs	No Access	**Read**	**Read, Write & Modify**	**Read, Write & Modify**	**Read, Write & Modify**	**Read, Write & Modify**	No Access
Students	DENY	**Read**	**Read & Write**	**Read, Write & Modify**	No Access	**Read & Write**	No Access
Visitor	No Access	DENY	DENY	No Access	No Access	No Access	No Access

2.2.4 Policies and guidelines for use of accounts

Users are expected to become familiar with and abide by LS policies, standards and guidelines for appropriate and acceptable usage of the network and systems.

2.2.5 Access for remote users

LS does not currently have a remote access option for its staff, the only remote access is currently granted to the ICT Officer via the Southend Borough Council IT Support Team. No uncontrolled remote access is permitted to any network device or system.

2.2.6 Physical access control

Physical access to sensitive areas and access to sensitive physical information must be tightly controlled.

2.2.6.1 Physical access to staff information

Physical access to staff data is limited to the Headteacher, the Headteacher's Personal Assistants and the School Administrator. All access has to be authorised by the Executive Headteacher.

2.2.6.2 Physical access to student data

Physical access to student academic and general education files are accessible by all LS staff but cannot leave the office.

Contact details for students are accessible by all LS staff but cannot leave the office.

Safeguarding information on the students is held in a separate location to other student information. This information is only accessible to the Headteacher and the Administrative Staff.

Comment [DW2]: Just need you to double check this

2.2.6.3 Physical access to financial data

Confidential financial records are stored in a location which is accessible to all Administrative Staff.

General financial information (such as orders and invoices) are accessible and authorised for all Administrative Staff.

Long term archive of all financial information is accessible by all Administrative Staff and Site Staff.

Comment [DW3]: Just need you to double check this

2.2.6.4 Physical access to governing body and trust information

Physical governing body and trust information is accessible by all Administrative Staff but access is only authorised for the Headteacher and the Headteacher Personal Assistants.

2.2.6.5 Physical access to admission information

Admission information (such as requests and denies) are accessible and authorised for all Administrative Staff and all Senior Management Team.

2.2.6.6 Physical access to network equipment

The servers are located in the comms room which remains locked when unoccupied. Authorised personnel are SBC Admins, IT Technician and Site Staff, no unauthorised personnel should be left unattended.

Comment [DW4]: Maybe we need to lock this room?

Access to the servers and switches is authorised for SBC Admins and IT Technician. All active servers and switches must remain in locked cabinets.

2.2.6.7 Physical access to server backups

All Administrative Staff and Senior Management Team have access to the server backups but only SBC Admin and IT Technician is authorised.

2.3 Access control methods

Access control methods include explicit logon to devices, database access rights, encryption and other methods as necessary.

Access control applies to all LS networks, servers, workstations, laptops, tablets and services run on behalf of LS.

2.3.1 Access control for Microsoft devices

All users have single sign on credentials for Microsoft Windows devices and email if necessary. These credentials ensure NTFS security permissions for files and folders, user account privileges, server and workstation access rights and the ability to audit. Access control to all computer files will be granted by security groups linked to roles as shown in Section 2.2.3.

2.3.2 Access control for iPads

All school iPads are controlled via a mobile device management system which sets restrictions and limitations. Password based access is enforced on all staff iPads.

Comment [DW5]: Currently no password but enforcing one might be tricky for students

2.3.3 Access control for the Wi-Fi network

While all devices have access to the Wi-Fi network, only SBC Admins and the IT Technician have access to the password.

Guests may be granted temporary access to the Wi-Fi network but must have settings removed when they leave the premises.

2.4 Cloud Systems

The use of cloud-based systems and databases by LS must meet the access control provisions laid out in this policy.

Access control is managed by the relevant resource leaders in LS.

2.5 Penetration tests

Regular penetration tests will be made to LS's access control provision to attain the effectiveness of existing control and expose any weakness.

2.6 Further Policies, Codes of Practices and Guidelines

This policy and other supporting documents will be made available in the school office and on the school website. All staff, students and any third parties authorised to access LS network are required to families themselves with this policy and other supporting documents and to adhere to them at all times.

Comment [DW6]: Do we need to put this policy on the website?

2.7 Review and Development

This policy shall be reviewed and updated regularly to ensure that it remains appropriate and relevant to any changes to the law or organisational policies.

Additional regulations may be created to cover specific areas.

3 Responsibilities

LS Staff:
All members of LS and third parties working for LS may have or require access to LS data or IT systems and therefore may be responsible for the systems which LS data resides.

School Administrator:
Responsible for access and control of physical data.

Network Manager:
Responsible for writing this policy and establishing access control on the computer network.

Site Staff:
Responsible for physical security on site

4 Document Control

Distribution list

- Public availability
- Executive Headteacher
- Administration Staff

External Document References

Date	Version	Comments
21/06/18	0.1	Initial draft

Review Control

Reviewer	Section	Comments	Actions Agreed