Leicester Partnership School

ICT Security Policy

Including

Internet and E-mail use

Version 1.0b

Schedule for Development, Monitoring and Review	
Approved by governors on:	18th March 2021
Implementation monitored by:	Clive Francis
Review arrangements:	Annually All policies will be reviewed if there are any significant developments or changes to legislation
Reviewed:	March 2023
The next review of this policy:	March 2024

Leicester Partnership School (LPS) – ICT Security Policy

Contents

1. Managing the Policy

1.1 Legislation and guidance

This policy meets the lawful requirements of and is influenced by the following Enacted Legislations:

- Protection of Children Act 1999
- Children Act 2004
- Data Protection Act 2018 (UK GDPR)
- The Communications Act 2003

1.2 Compliance

- This policy sets out Leicester Partnership School's obligation in relation to all aspects of Information and Communications Technology and applies to all employees, including those employed on a temporary or contract basis.
- Anyone who is found to have breached this policy could be subject to Leicester Partnership School's Disciplinary and Dismissal Policy & Procedure and serious breaches of this policy could be regarded as gross misconduct.
- If you do not understand the implications of this or how it may apply to you, seek advice from Human Resources.

1.3 Advice and Training

If you do not understand anything in this policy or feel you need specific training to comply with it you should bring this to the attention of your manager.

2. Introduction

Presently, the Leicester Partnership School (LPS) works with a number of permanently excluded students with a range of specialist needs.

The Leicester Partnership School will:

- Ensure students have the opportunity to use ICT and have the necessary skills to utilise it
- To openly encourage and assist staff to promote the use of ICT
- Provide training and support for staff by identifying needs and providing opportunities for training

3. Purpose and Objectives

The Policy provides guidance to employees on all aspects of information and communications technology and brings together the following policies:

- E-safety policy (online safety and acceptable use)
- Email Policy

- Internet Policy
- Portable Devices Policy (Including Removable Media)
- Security (Password Policy)
- Authorised user Policy

Its aims are:

- Develop confidence and competency in the use of computers and related hardware in a range of contexts and with a cross curricular approach.
- Develop an understanding of the contribution that ICT can make to solving problems in a systematic and methodical manner.
- Develop knowledge about the application and use of various ICT tools in society.
- Acquire awareness of the importance and limitations of such ICT tools and use these tools effectively.
- Understand the opportunities ICT can provide and appreciate the effects and limitations of ICT.

4. Roles and Responsibilities

- The ICT Network Manager is responsible for the provision of appropriate technology and technological devices to ensure the efficient and effective working of LPS.
- All employees, whether temporary or contract are responsible for ensuring they are familiar with all aspects of this policy, particularly relating to the security of information or devices.
- Misuse of the ICT systems and network can have serious consequences both for LPS and individuals.

5. Security

5.1 Passwords

- Each user is issued with an individual Identification (user ID) and a Password, which enables appropriate access to the network and software systems. The use of IDs and Passwords offers security to the LPS system itself and importantly to the data retained on the system.
- Your password does not imply personal privacy, as LPS has ICT Administrative accounts which have access to all user areas. Unless express permission is given by the user, only authorised staff in the ICT team will access these areas.
- IDs and Passwords are important - they give access to the network and software and give the user the rights needed to save and access data in the Directory system, whilst protecting the data from inappropriate users.
- Users should not let anybody else have access to their ID and Password unless specifically requested to do so by their line manager or senior management.
- Users may be prompted to save their passwords when accessing some websites on a web browser, this is only secure to do so when signed into their own account. Do not save passwords for websites when using a shared account i.e. the visitor's account, this may give unauthorised users access to your accounts ID and password.
- The ICT team controls the regulation of user accounts and passwords implementing a strict policy of minimum length, maximum age of 365 days and password complexity. When selecting a password users should ensure it is strong and follow these guidelines:
    - Minimum password length 8 characters, including upper case, numbers and a special character.
    - Not a single long word as found in any dictionary

- Use 3 short random words together with a number and special character.
- Not based on personal information, e.g. names, dates etc.

- The system will request that users specify a different password each time they change it. Users will not be allowed to reuse the last 5 previous passwords.
- User accounts will be locked out after 5 incorrect login attempts. The user account will be unlocked after a 10-minute period or by an authorised IT administrator.

5.2 Network

- Users may have the ability to connect to other user areas on network drives, depending on the permissions granted. This does not give the user the authority to read, alter or copy other users' files - unless they have permission.
- Users should always ensure that their computer/laptop account is logged out of or locked when it is left unattended. Failure to do this directly affects the security of the LPS network e.g. by potentially allowing an unauthorised person to access LPS systems and/or data. This would then also be a data breach according to the UK General Data Protection Regulation (UK GDPR)

5.3 SIMS Database

- Software for the Schools MIS database (SIMS) is not automatically governed by the same account name and password that governs network security. However, the passwords must be treated by users in the same way with care to ensure the security of the password being the main governing feature.
- User IDs and passwords for SIMS will be generated by the SIMS manager and an email sent to the user confirming their details. It is the responsibility of the user to keep this secure at all times.
- You must change your SIMS password at least once a year.
- Never leave the SIMS database logged in when not at your computer (see network security).

5.4 Portable Devices

- Laptops and all other portable devices capable of storing data, including mobile phones and USB memory sticks, are issued for work purposes only and should be treated as such.
- No unauthorised home usage, e.g. additional software can be loaded or the device altered physically in any way. Any unauthorised software found by the ICT Team will be removed immediately.
- Personally owned storage equipment such as memory sticks or external drives should not be used or connected to any company equipment at any time.
- Personally owned SD cards (memory cards) shall not be used in any company equipment e.g. cameras at any time.
- Only encrypted removable storage devices may be used, unless explicit permission is granted by the ICT Network Manager, and must be scanned for viruses.
- Authorised users may be assigned an encrypted removable storage device, it is the user's responsibility to ensure the security of the encryption key and any data taken outside of the school's network.
- In the event of a theft or breakage staff involved will report all relevant details to their Line Manager and ICT team immediately, who will then inform the Business Manager. The Business Manager will direct the ICT Network Manager to specify and procure any replacement equipment. Preventative/corrective action will be taken based on lessons derived from incidences of theft.

5.5 Security Breach

- A breach or suspected breach of policy by a School employee, contractor or student may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.
- Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure.
- Policy breaches may also lead to criminal or civil proceedings.

5.6 Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the ICT Network Manager.

6. Emails

This policy applies to all emails prepared and sent from the LPS's email addresses or mailboxes and any non-work email sent using the LPS's ICT facilities.

6.1 Email as Records

- All emails that are used to conduct or support official LPS business must be sent using an "@lps.leicester.sch.uk" address.
- Non-work email accounts must not be used to conduct or support official LPS business.
- All emails that represent aspects of LPS business or administrative arrangements are the property of LPS and not of any individual employee.
- Emails held on LPS equipment are considered to be part of a corporate record and may also provide a record of employees' activities. The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official LPS business should be considered to be an official communication from LPS. To ensure that LPS is protected adequately from misuse of e-mail, the following controls will be exercised:
    - It is a condition of acceptance of this policy that users comply with the guidance provided as part of staff induction.
    - Some official external e-mails may include one or more of the following disclaimers:
        - *'Data Protection – personal data you provide to LPS will be processed in line with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018. For more information on how your information is used; how we maintain the security of your information and your rights, including how to access information that we hold on you and how to complain if you have any concerns about how your personal details are processed, please see consult our Data Protection Policy.'*
        - *'This Email, and any attachments, may contain Protected or Restricted information and is intended solely for the individual to whom it is addressed. It may contain sensitive or protectively marked material and should be handled accordingly. If this Email has been misdirected, please notify the author immediately. If you are not the intended recipient you must not disclose, distribute, copy, print or rely on any of the information contained in it or attached, and all copies must be deleted immediately. Whilst we take reasonable steps to try to identify any software viruses, any attachments to this Email may nevertheless contain viruses which our anti-virus software has failed to identify. You*

should therefore carry out your own anti-virus checks before opening any documents. LPS will not accept any liability for damage caused by computer viruses emanating from any attachment or other document supplied with this e-mail.'

- Whilst respecting the privacy of authorised users, LPS maintains its legal right to monitor and audit the use of email by authorised users to ensure adherence to this Policy. Users should be aware that the deletion of e-mails from individual accounts does not necessarily result in permanent deletion from the LPS IT systems.
- It should also be noted that emails and attachments (whether sent or received) may need to be disclosed under the UK GDPR, the Data Protection Act 2018 or the Freedom of Information Act 2000. Further information regarding this can be obtained from the Information Governance Officer.

6.2 Email as a Form of Communication

- Email is designed to be an open and transparent method of communicating. However, it cannot be guaranteed that the message will be received or read, nor that the content will be understood in the way that the sender of the email intended. It is therefore the responsibility of the person sending an email to decide whether email is the most appropriate method for conveying time-critical or OFFICIAL SENSITIVE information or of communicating in the particular circumstances.
- Email in general is not a secure method of communication. Therefore, all staff should carefully consider whether email is the most appropriate method to use. If necessary, personal or confidential information should be sent as a password-protected attachment, with the password being communicated verbally to the recipient.
- When communicating via email, staff are expected to adhere to email etiquette:
    - Is the email really necessary or would a conversation be better?
    - Only send emails and expect replies during the working day
    - Don't send the email to all staff unless absolutely necessary
    - Avoid writing emails when upset or angry as it may be conveyed in your words.
    - Lengthy emails should be avoided, try and keep the message short and to the point.
    - Continue thread conversations – it keeps email inboxes cleaner
    - Add NRN (No Response Necessary) to your email if you don't expect or require a response
    - Don't neglect the subject line – keep it short and relevant to the email content
    - Make sure you are sending the email to the correct recipients
    - Always proofread the email before sending

6.3 Junk Email

- There may be instances where a user will receive unsolicited mass junk email or spam. It is advised that users delete such messages without reading them. Do not reply to the email. Even to attempt to remove the email address from the distribution list can confirm the existence of an address following a speculative e-mail.
- Before giving your e-mail address to a third party, for instance via a website, consider carefully the possible consequences of that address being passed (possibly sold) on to an unknown third party, and whether the benefits outweigh the potential problems.
- Chain letter e-mails (those that request you forward the message to one or more additional recipients who are unknown to the original sender) must not be forwarded using LPS systems or facilities.

6.4 Confidentiality

- All employees are under a general requirement to maintain the confidentiality of information which they may have access to as part of their role. There are also particular responsibilities under Data Protection legislation to maintain the confidentiality of personal data. If any employee is unsure of whether they should pass on information, they should consult the Information Governance Officer.
- Staff must make every effort to ensure that the confidentiality of email is appropriately maintained. Employees should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies. Moreover, confidentiality cannot be assured when messages are sent over external networks, such as the internet, because of the insecure nature of such networks and the number of people to whom the messages can be freely circulated without the knowledge of LPS.
- Care should be taken when addressing emails to prevent accidental transmission to unintended recipients. Particular care should be taken if the email client software auto-completes an email address as the user begins typing a name.

6.5 Negligent Virus Transmission

- Computer viruses are easily transmitted via email and internet downloads. Full use must therefore be made of LPS's anti-virus software. If any user has concerns about possible virus transmission, they must report the concern to ICT Support.

In particular, users must:

  - Not transmit by email any file attachments which they know to be infected with a virus.
  - Not download data or programs of any nature from unknown sources.
  - Report any suspected files to ICT Support.
  - Report any email security incidents to ICT Support.

6.6 Personal Use

- You are <u>not</u> permitted to use your LPS email account to send personal emails. Access to other providers of email, for example, Outlook, Gmail etc. is through the internet and therefore only allowed subject to the conditions of Personal Use of the internet in section **7.1** of this policy.

7. Internet

- The Internet service is primarily provided to give LPS staff and authorised users access to relevant information for the purpose of conducting their intended function for the business and to the benefit of students and colleagues.
- All internet activity is logged by the school's internet provider (KCOM/NASSTAR) and the internet filtering service provider (ekte). These logs may be monitored by authorised staff.

7.1 Business and Personal Use of Internet Facilities

- LPS will seek to ensure that the Internet and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

- LPS expects all staff and pupils to use the Internet and digital technologies responsibly and strictly according to current policy. These expectations are also applicable to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.
- Access to the Internet for personal use must be confined to outside of normal working hours. Personal use must still comply with this policy including its provisions regarding misuse.

7.2 Things You Must Not Do

- Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - Indecent images of children
  - Promoting discrimination of any kind
  - Promoting racial or religious hatred
  - Promoting illegal acts
  - Any other information which may be offensive to peers or colleagues e.g. abusive images; promotion of violence; gambling; criminally racist or religious hatred material
  - Hacking
  - Weaponry
- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.
- Subscribe to, enter or utilise real-time chat facilities such as chat rooms, text messenger or pager programs.
- Subscribe to, enter or use online gaming or betting sites.
- Subscribe to or enter "money making" sites or enter or use "money making" programs.
- Run a private business.
- Download any software without prior authorisation from IT.

The above list gives examples of "unsuitable" usage but is neither exclusive nor exhaustive. "Unsuitable" material would include data, images, audio files or video files the transmission of which is illegal under British law, and, material that is against the rules, essence and spirit of LPS and its policies. If you inadvertently access a blocked internet site you must report this to ICT Support.

LPS recognises that in certain planned curricular activities, access to otherwise considered inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded and also that permission is given by senior leaders so that the action can be justified if queries are raised later.

- Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:
  - Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative).
  - Adult material that potentially breaches the Obscene Publications Act in the UK.
  - Criminally racist or anti-religious material.
  - Violence and bomb-making.
  - Illegal taking or promotion of drugs.
  - Software piracy.
  - Other criminal activity.

7.3 Responsibilities

- It is all users' responsibility to assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.
- It is the responsibility of Line Managers to ensure that the use of the Internet facility within an employee's work time is relevant to and appropriate to LPS business and within the context of the user's responsibilities. Also within employee's own time is subject to the rules contained within this policy.
- Where KCOM (provider of Internet connectivity and associated services to schools) and/or emPSN become aware of an illegal act or an attempted illegal act, they will have to comply with the law as it applies and will take action directed by the police if a Regulation of Investigatory Powers Act (RIPA) Notice is issued.

8. Anti-Virus, malware and Ransomware

LPS is very proactive in managing potential computer virus/malware/ransomware attacks. All company systems are protected by centrally administered Sophos Intercept X software which also helps protect against malware and ransomware attacks. The software automatically updates and scans all computers daily. E-mail is also filtered and scanned for viruses utilising this software.

Virus Infection

- Any staff member found to be knowingly introducing a virus to the network system will be subject to disciplinary procedure, which depending on the severity of the incident could lead to dismissal.
- All network computers will be updated with anti-virus software by the ICT systems, users of laptops must ensure they connect the laptop to the network at least once a week to maintain the anti-virus software.
- Never interfere with any anti-virus software installed on school ICT equipment that you use.

9. Disposal of Redundant Equipment

All redundant ICT equipment will be disposed of through an authorised agency in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA). This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.