Lindridge St Lawrence CE VA Primary School and Nursery

'Discovering life in all its fulness', John 10.10b

Data Security and Protection Policy
Academic Year: 2024–25

1. Introduction

This policy outlines how we securely process, store, and handle data at Lindridge St Lawrence CE Primary School. It applies to all staff and anyone accessing school IT systems. Everyone is responsible for keeping data safe and secure.

2. What Is Data Security?

Data security means protecting personal information — whether on paper or electronically — from unauthorized access. Personal data includes:

- Names, contact details, gender, date of birth
- Academic progress, achievements, attendance, behaviour
- Sensitive information about pupils and families

The biggest risk to data security is how users manage it — which means all staff must follow best practices.

3. Passwords

To protect sensitive data, staff must:

- Use strong, secure passwords

- Never share or write down passwords
- Log out or lock screens when leaving devices unattended
- Avoid using work passwords for personal accounts
- Never save passwords in browsers or send them via email or messaging
- Keep devices secure at all times

4. Data Protection

Staff must follow the **Data Protection Act** and the school's **Acceptable Use Policy**. Key rules include:

- Never copy sensitive data to unauthorized devices (e.g. USBs, home PCs)
- Keep data accurate, relevant, and up to date
- Secure and back up master documents
- Properly delete sensitive data (including emptying the Recycle Bin)
- Treat mobile devices with the same care as desktop computers

5. Equipment Security

- Devices with sensitive data must be encrypted
- Staff are responsible for school-issued equipment
- Never loan devices to others (including family)
- Keep laptops and USBs secure at all times
- Do not leave devices in vehicles — even in the boot
- Staff laptops must connect to the school network at least once per half term for updates

6. Other Good Practices

- Always shut down computers properly — avoid standby or sleep modes
- Be aware of others watching when entering passwords or viewing sensitive data
- Use secure storage when travelling (e.g. hotel safes)
- Keep remote access tokens separate from laptops

- Avoid public Wi-Fi for accessing school systems

School equipment is for use by **authorized school users only**.

7. Records and Documents

- Sensitive documents (e.g. safeguarding, staff and pupil files) must be stored in locked cabinets with restricted access
- SEND files are stored in a locked cupboard in the Headteacher's office
- Archived documents must be stored securely

8. Retention, Destruction & Archiving

- Follow current guidelines for document retention
- Shred sensitive documents when no longer needed
- Child protection files must be copied before transfer to another school, signed for, and a copy retained
- Archived files are stored securely in the Headteacher's office or designated cupboard

Approved by: Amanda Greenow-Langford

Date: 27.09.2025

Last Reviewed: 27.09.2025

Next Review Due: 27.09.2026