



Information Security Policy

Approval Date: September

Review Date: July 2027

Responsible Officer: Headteacher

Data Protection Officer: Warwickshire Data Protection Officer

1. Purpose

Galley Common Infant School is committed to protecting the confidentiality, integrity and availability of all information it holds.

This policy sets out the responsibilities of all staff, governors, volunteers, contractors and anyone working on behalf of the school in ensuring information is handled securely and in accordance with:

- UK General Data Protection Regulation (UK GDPR)
 - Data Protection Act 2018
 - Freedom of Information Act 2000
 - Keeping Children Safe in Education (KCSIE)
 - Records Management guidance
 - Warwickshire County Council information governance requirements where applicable.
-

2. Scope

This policy applies to:

- Employees
- Temporary staff
- Supply staff
- Volunteers
- Governors
- Contractors
- Third-party service providers acting on behalf of the school

All users of school information systems are responsible for protecting information assets.

3. Information Security Principles

The school will ensure that personal data is:

1. Processed lawfully, fairly and transparently.
2. Collected for specified, explicit and legitimate purposes.
3. Adequate, relevant and limited to what is necessary.
4. Accurate and kept up to date.
5. Retained only as long as required.
6. Processed securely to protect against unauthorised access, loss, destruction or damage.

The school will additionally ensure information remains:

- Confidential
 - Accurate
 - Available when required
 - Protected from cyber threats and unauthorised disclosure.
-

4. Roles and Responsibilities

Governing Board

The Governing Board is responsible for ensuring suitable information governance arrangements are in place and monitored.

Headteacher

The Headteacher is responsible for:

- Implementing this policy.
- Ensuring staff receive appropriate training.
- Managing information security incidents.
- Ensuring appropriate technical and organisational security measures are in place.

Data Protection Officer

The DPO provides advice and monitoring regarding compliance with data protection legislation.

All Staff

All staff must:

- Comply with this policy.
 - Complete required data protection and cyber security training.
 - Report incidents immediately.
 - Protect school information and systems.
-

5. Information Classification

Information should only be accessed by those with a legitimate business need.

Particular care must be taken with:

- Pupil records
 - SEND information
 - Safeguarding records
 - Staff personnel files
 - Medical information
 - Behaviour records
 - Financial information
-

6. Information Storage and Management

Paper Records

Staff must:

- Operate a clear desk approach.
- Store confidential records in locked cabinets.
- Remove documents promptly from printers.
- Use confidential waste disposal facilities.
- Retain records in accordance with the school's retention schedule.

Electronic Records

Staff must:

- Use only approved school systems.
 - Store records within authorised cloud services and network storage.
 - Not store confidential data on personal devices or unapproved systems.
 - Lock devices when unattended.
 - Use strong passwords and multi-factor authentication where available.
 - Never share accounts or passwords.
-

7. Email and Digital Communications

Staff must:

- Verify recipient details before sending information.
- Use BCC when emailing groups externally.
- Take care when opening unexpected emails, links or attachments.
- Use approved secure methods when sending confidential or special category data.
- Never forward school information to personal email accounts.

Sensitive personal information must only be shared where there is a lawful basis and appropriate safeguards in place.

8. Information Sharing

Information sharing must:

- Have a lawful basis.
- Support safeguarding, education or operational purposes.
- Be proportionate and necessary.
- Be documented where appropriate.

Where personal information is shared routinely with another organisation there must be an appropriate contract, Data Processing Agreement or Information Sharing Agreement in place.

9. Remote and Mobile Working

Staff working away from school must:

- Use school-issued devices wherever possible.
- Connect through secure networks.
- Keep paper files secure and out of sight.
- Ensure family members and others cannot access school information.
- Not leave devices or confidential information unattended.
- Report loss or theft immediately.

Confidential information must not be stored permanently at home.

10. Physical Security

The school will maintain appropriate physical security measures including:

- Visitor sign-in procedures.
- ID badges where applicable.
- Secure storage for records.
- Controlled access to staff-only areas.

All staff must challenge or report unknown individuals on site where appropriate.

11. Portable Media and Devices

The use of USB drives and other removable media should be minimised.

Where removable media is required:

- Encryption must be used.
 - Only approved devices may be used.
 - Personal devices must not be used to store school data.
 - Information should be transferred to approved school storage as soon as possible.
-

12. Cyber Security and Malware Protection

The school will maintain appropriate cyber security controls including:

- Anti-malware protection.
- Security updates.
- Access controls.
- Filtering and monitoring systems.
- Secure backups where appropriate.

Users must not:

- Install unauthorised software.
- Disable security controls.
- Circumvent security arrangements.

Any suspected malware or phishing attempt must be reported immediately.

13. Access Control

Access to systems will be granted according to business need and the principle of least privilege.

The school reserves the right to:

- Monitor system use.
- Remove access rights.
- Investigate suspected misuse.

Users must:

- Log out when leaving devices unattended.
 - Protect passwords and authentication methods.
 - Never use another person's account.
-

14. Monitoring

The school may monitor the use of its systems, devices and networks for:

- Security purposes.
- Safeguarding purposes.
- Compliance with statutory obligations.

Monitoring will be lawful, proportionate and carried out in accordance with relevant legislation.

15. Information Security Incidents and Data Breaches

All actual or suspected information security incidents must be reported immediately to the Headteacher and Data Protection Officer.

Examples include:

- Lost or stolen devices.
- Information sent to the wrong recipient.
- Unauthorised access to records.
- Malware infections.
- Cyber attacks.
- Loss of paper records.

Where required, breaches will be assessed and reported to the Information Commissioner's Office (ICO) in accordance with legal requirements.

16. Non-Compliance

Failure to comply with this policy may result in disciplinary action and, where appropriate, referral to external authorities.

Review

Next Review Date: July 2027

Approved By: Governing Board
