Rainow Primary School

Caring, Learning, Achieving.

Data Security Breach Prevention and Management Plan

Members of staff responsible: School Business Manager/Headteacher
Date approved by the governors: Spring 2026
Date to be reviewed: *Spring 2029

Contents

Statement of intent

Rainow Primary School is committed to maintaining the confidentiality, integrity and availability of its information and ensuring that details of finances, operations and individuals within the school are only accessible to appropriate, authorised individuals.

We recognise that the majority of information is now stored online or on electronic devices, and that schools are increasingly the target of cyber-attacks and social engineering (e.g. phishing emails, scam phone calls). It is therefore essential that we:

- Uphold high standards of information security.
- Take suitable technical and organisational precautions.
- Maintain clear systems and procedures that support prevention, detection, response and recovery.

Where a security breach does occur, the school will:

- Act promptly to contain and investigate the breach.
- Minimise the potential negative impact on pupils, staff and the wider school community.
- Notify relevant authorities and individuals where required.
- Learn lessons and improve systems to reduce the likelihood and impact of any repeat occurrence.

For the purposes of this policy:

The “data controller” refers to the organisation with overall responsibility for deciding how and why personal data is used (usually the local authority, the governing body or both jointly, depending on local arrangements).

The school’s named data protection lead (referred to here as the “Data Controller” role for simplicity) is the person within school with day-to-day responsibility for overseeing data protection and information security.

Where a Data Protection Officer (DPO) is appointed under UK GDPR (e.g. via the local authority or external provider), they will advise on, and be consulted about, breaches of personal data.

1. Legal framework

1.1 This policy has due regard to statutory legislation, regulations and guidance, including, but not limited to, the following:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Computer Misuse Act 1990
- Freedom of Information Act 2000 (where relevant to information security)
- Privacy and Electronic Communications Regulations (PECR) (for electronic communications)
- Relevant guidance from the Information Commissioner's Office (ICO) and the National Cyber Security Centre (NCSC)

1.2 This policy has due regard to the school's policies and procedures including, but not limited to, the following:

- Data Protection Policy
- E-Safety / Online Safety Policy
- Acceptable Use Policy (AUP)
- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Records Management / Retention Schedule

2. Types of security breach and causes

2.1 Unauthorised access without damage to data

An unauthorised person accesses data on the school system (e.g. a "hacker") who may read or copy data, but does not alter or delete it.

2.2 Unauthorised removal or disclosure of data

An authorised person accesses data and removes or shares it with an unauthorised person, e.g. a staff member with authorised access who passes data to a friend, stores it on an unauthorised personal device, or uploads it to unapproved cloud storage. This is also known as data theft or unauthorised disclosure.

2.3 Damage to physical systems

Damage to the hardware in the school's ICT system, such as theft, fire, flood, vandalism or hardware failure, which may result in data being inaccessible to the school and/or becoming accessible to unauthorised persons.

2.4 Unauthorised damage to data

An unauthorised person or malicious software (e.g. ransomware, viruses) alters, encrypts or deletes data.

2.5 Breaches in security may be caused by individuals, accidentally, maliciously or through negligence. Examples include:

Accidental breaches, e.g.

- Sending an email with personal data to the wrong recipient.
- Losing a laptop, USB stick or paper file containing personal data.
- Insufficient training so staff are unaware of correct procedures.
- Malicious breaches, e.g.
- A hacker or disgruntled insider wishing to cause damage through accessing, altering, sharing or removing data.
- Deliberate installation of unauthorised software.
- Negligence, e.g.
- Leaving systems logged in and unattended.
- Using weak or shared passwords.
- Ignoring school policies and procedures.

2.6 Breaches may also be caused by system issues, such as incorrect installation, configuration problems or operational errors. Examples include:

- Incorrect installation or configuration of anti-virus or endpoint protection software.
- Out-of-date systems or software no longer supported by suppliers.
- Incorrect firewall or filtering settings, allowing unintended access to the network.
- Confusion between backup copies of data, leading to overwriting live data or losing the most recent version.

3. Roles and responsibilities

3.1 The Headteacher is responsible for:

- Implementing effective strategies for the management of risks posed by ICT and internet use.
- Ensuring the school keeps its network services, data and users secure.
- Ensuring that this policy and associated procedures are implemented and resourced.

3.2 The Data Controller role / school data protection lead is responsible for:

- Overall monitoring and management of data security and personal data breaches.
- Liaison with the DPO (if appointed), local authority and external advisers where appropriate.
- Ensuring that personal data breach notifications are made to the ICO and affected individuals where required.

3.3 The Headteacher is responsible for ensuring a clear procedure exists for managing and logging security incidents.

3.4 The Computing Lead, supported by the school's sub contracted IT Technician, is responsible for:

- Managing pupils' log-ins and their use of the internet within school.
- Supporting staff in following the Acceptable Use Policy and Online Safety Policy.

3.5 The IT Technician (*School ICT Support*) is responsible for:

- Installing and maintaining software within school.
- Managing passwords and access rights to data and systems.
- Monitoring usage and filtering reports in conjunction with the Computing Subject Leader.
- Checking and managing backups and technical disaster recovery arrangements.

3.6 The governing body is responsible for:

- Holding meetings with the Headteacher and data protection lead to discuss data and cyber security.
- Reviewing incident logs and ensuring that appropriate controls, resources and training are in place.

3.7 All members of staff and pupils are responsible for:

- Adhering to this policy, the Data Protection Policy, E-Safety / Online Safety Policy and Acceptable Use Policy.
- Reporting any suspected or actual security breach immediately in line with section 12.

4. Secure configuration

4.1 An up-to-date inventory will be kept of all IT hardware, software, operating systems and cloud-based services in use at the school. This will be stored on the server or a secure shared location and audited periodically.

4.2 Any changes to hardware, software or cloud services will be documented in the inventory, including:

- Installation of new systems or applications.
- Application of major updates, patches or configuration changes that may affect security.

4.3 Any software or operating systems that are out of date or have reached "end of life" will be removed from systems or fully isolated, and replaced or upgraded where necessary.

4.4 All hardware, software and operating systems will require unique user accounts and strong passwords for individual users before use. Where possible,

key systems (e.g. MIS, email, cloud services) will use multi-factor authentication (MFA).

4.5 Default passwords on devices and systems will be changed upon installation. Administrative accounts will be restricted and only used when necessary.

4.6 The school recognises that locking down hardware and software is an effective way to prevent access by unauthorised users and to limit the impact of any compromise.

5. Network security

5.1 The school will employ firewalls, web filtering and appropriate network segmentation to prevent unauthorised access to systems.

5.2 The school's firewall is deployed as:

- A centralised deployment: the broadband service connects to a firewall located within a data centre or other major network location and/or at the school perimeter, managed by School's Broadband.

5.3 As the firewall is managed by a third party, the IT Technician will ensure that:

- Any changes and updates requested by authorised users are implemented promptly.
- Security patches and fixes are applied in a timely way.
- Appropriate filtering and monitoring settings are in place for an educational environment.

5.4 Network equipment (e.g. switches, wireless access points) will be configured securely, with management interfaces restricted to authorised staff and strong authentication in place.

6. Malware prevention

6.1 The school understands that malware (including viruses, spyware, ransomware and other malicious code) can be damaging for network security and can enter the network through email attachments, websites, removable media, social engineering and other means.

6.2 The IT Technician will ensure that:

- All school devices have centrally-managed and up-to-date anti-malware / endpoint protection.
- Regular malware scans are carried out and logged.
- Only authorised personnel can alter malware controls.

6.3 Malware protection updates, including signatures and program updates, are set to happen automatically wherever possible.

6.4 Malware protection and other security controls will also be reviewed and updated after any incident to ensure they remain effective.

6.5 Web filtering, as detailed in section 7, will ensure that access to websites with known malware or inappropriate content is blocked and logged.

6.6 The school will use email security technology (e.g. spam and phishing filters, attachment scanning) to detect and block malware and suspicious messages.

6.7 School's ICT Support will periodically review mail and web security controls to ensure they remain up-to-date and effective.

7. User privileges

7.1 The school will operate on the principle of least privilege. User accounts will be configured so that:

- Users only have access to the systems and data they need to perform their role.
- Administrative privileges are restricted and closely controlled.

7.2 The Headteacher will clearly define user access profiles (e.g. pupil, teacher, admin staff, senior leader) and communicate these to the Data Controller role and IT Technician, ensuring a written record is kept.

7.3 The Data Controller role and IT Technician will ensure that user accounts and group memberships are set up in line with these profiles, to minimise the potential for accidental or deliberate misuse.

7.4 Filtering and monitoring reports are produced regularly (e.g. daily/weekly) and checked by the IT co-ordinator for inappropriate or malicious content. Any member of staff or pupil who accesses such content will be recorded and dealt with under the appropriate behaviour or disciplinary procedures.

7.5 Pupils are responsible for keeping their passwords secure. The IT Technician can reset passwords where necessary, following identity verification.

7.6 A generic user ID and password may be used for Reception and Key Stage 1 pupils where appropriate. All pupils also have, or will progressively receive, individual logins as they move through school, allocated by the IT Technician following a request from the IT co-ordinator.

7.7 The "master user" or administrative password used by the IT Technician will be made available, in a sealed or secure format, to the Headteacher or other nominated senior leader for emergency use only.

7.8 The Data Controller role, in conjunction with the IT Technician, will ensure that accounts for staff, contractors and volunteers who have ceased employment or no longer require access are promptly disabled and then deleted.

8. Monitoring usage

8.1 Monitoring user activity is important for early detection of attacks, inappropriate behaviour and potential data breaches.

8.2 The school will inform all staff, pupils and visitors that their use of school ICT systems, devices, email and internet may be monitored and logged, in accordance with the Acceptable Use Policy and Online Safety Policy.

8.3 If a user accesses inappropriate content or a potential threat is detected:

- An alert will be generated by the filtering/monitoring system.
- Alerts will be sent to the Headteacher, Deputy Headteacher, Computing Subject Leader, School Admin in line with agreed thresholds.

8.4 Alerts will identify:

- The user (or device) involved.
- The activity that prompted the alert.
- The information or service the user was attempting to access.

8.5 The IT Technician and Computing Subject Leader will review suspicious activity and report concerns to the Headteacher and Data Controller role. Incidents will be responded to in accordance with section 12 and the Online Safety Policy.

8.6 Monitoring data will be retained for an appropriate period in a secure location and may be used:

- As evidence in the investigation of a suspected breach.
- To check that systems are functioning correctly.
- To support continual improvement of security controls.

9. Home working

9.1 The IT Technician will ensure that all school-owned laptops and other portable devices are encrypted and password protected. If such devices are lost or stolen, this will help prevent unauthorised access to personal data.

9.2 Staff should not use personal devices to access school systems or personal data where the school provides suitable alternatives (e.g. work laptops), unless authorised by the Headteacher.

9.3 Where staff are authorised to use personal devices, they must:

- Ensure the device has up-to-date anti-malware and firewall protection.
- Use strong passwords, screen locks and, where possible, encryption.
- Only access school systems via approved secure methods (e.g. VPN, secure cloud platforms).
- Not store school data permanently on personal devices or personal cloud services.

The IT Technician may check personal devices used for work purposes to confirm that they meet minimum security requirements.

9.4 The Headteacher will determine the limitations on remote access to the network, balancing security and operational needs.

9.5 Staff using school-owned laptops or tablets will use them for work purposes only, whether on or off school premises, in line with the Acceptable Use Policy.

9.6 The school will use device tracking technology where possible to help locate lost or stolen equipment (currently applies to iPads and other supported devices).

9.7 Data will be stored centrally on school servers or approved cloud platforms (e.g. Schldocs, Arbor, RBUSS) to reduce the creation of multiple, uncontrolled copies.

9.8 The school Wi-Fi network will be password protected and segmented where possible (e.g. staff, pupil and guest networks). Access will only be granted as required.

Staff and pupils must not use the staff or pupil Wi-Fi for personal devices unless authorised by the Headteacher.

Guest / visitor access will be limited and will not allow access to Staffshare, Schldocs or other internal data stores.

10. Backing-up data

10.1 All electronic data held by the school will be backed up regularly. As a minimum:

- Onsite backups will be taken daily onto an encrypted onsite device (e.g. USB drive or backup appliance). Each backup will be retained for at least two weeks before being overwritten or deleted.
- Schldocs and Arbor will also be backed up remotely using RBUSS or equivalent approved cloud-backup services.

10.2 Backups will be tested periodically to ensure that data can be successfully restored.

10.3 Only authorised personnel will be able to access backup data.

11. User training and awareness

11.1 The IT co-ordinator or Headteacher will arrange age-appropriate training for pupils to ensure they use the network safely and responsibly, in line with the Acceptable Use Policy and Online Safety Policy.

11.2 All staff will receive regular training and updates (e.g. at least annually and after any significant incident or system change) covering:

- Basic data protection and information security.
- Recognising phishing and social engineering.
- Safe handling of personal data.
- Password and account security.
- Reporting procedures for suspected breaches.

11.3 Through training, all staff will know:

Who to inform immediately if they suspect a security or personal data breach.

Who to contact if they suspect someone else is using their account or password.

11.4 All new staff will receive information security and data protection training as part of their induction.

11.5 All users will be made aware of the disciplinary procedures for misuse of the network, devices or data, including malicious attacks or serious breaches, in accordance with the Acceptable Use Policy and staff/pupil behaviour policies.

12. Security breach incidents

12.1 Any individual who discovers or suspects a security or personal data breach must report this immediately to the Headteacher and the Data Controller role (and/or DPO where applicable).

12.2 When an incident is raised, the Headteacher or Data Controller role will complete a Security Breach Incident Form, recording as a minimum:

- Name and contact details of the individual who discovered the incident.
- Date and time the incident was discovered.
- Description of the incident (what happened, how it was detected).
- Description of any perceived or actual impact.
- Description and identification codes of any devices or systems involved.
- Location of the equipment involved.
- Any immediate containment actions taken.

12.3 The Data Controller role will lead the investigation and will be allocated sufficient time and resources.

12.4 The Data Controller role will quickly assess the severity of the breach and whether any personal data has been compromised.

12.5 The Data Controller role, in conjunction with the IT Technician, IT co-ordinator and other relevant staff, will oversee a full investigation and produce a written report.

12.6 The investigation will identify:

- The cause of the breach.
- Whether it has been fully contained.
- Whether further loss, damage or unauthorised disclosure is likely.

12.7 If the severity of the security breach is assessed as low (e.g. contained quickly, limited data involved, unlikely to pose a risk to individuals), the incident will be managed by:

Recording it in the incident log.

Taking any proportionate local remedial action (e.g. password reset, reminder training).

Applying appropriate disciplinary sanctions if necessary.

Making relevant technical or procedural adjustments to reduce the chance of recurrence.

12.8 Where possible, steps will be taken to recover lost or damaged data, using backups or other recovery tools.

12.9 Where the breach poses a higher risk, particularly where personal data or key systems are involved, the school will:

- Inform relevant staff of their roles and responsibilities in containment and recovery.

- Consider taking affected systems offline.
- Attempt to retrieve any lost, stolen or otherwise unaccounted-for devices or data.
- Restrict access to systems to a small group, if necessary.
- Back up remaining data and ensure it is stored safely.
- Review and, where necessary, strengthen basic security measures, including:
- Resetting passwords and login details.
- Ensuring physical access to server rooms and record storage areas is locked and controlled.

12.10 Where appropriate (e.g. where there is evidence of hacking, theft, fraud or criminal damage), the Data Controller role, in consultation with the Headteacher and DPO (if applicable), will inform the police or other relevant authorities.

12.11 The Data Controller role, IT co-ordinator and IT Technician will test affected systems before returning them to normal use. The incident will only be deemed resolved when the school is satisfied that systems are safe and stable.

13. Assessment of risks

13.1 To assess the risks arising from a breach, the Data Controller role will consider, and record in the investigation report, as many of the following questions as are relevant:

- What type and how much data is involved?
- How sensitive is the data? For example:
  - Special category personal data (e.g. health, SEND, ethnicity, religion) under UK GDPR.
  - Financial information (e.g. bank details).
  - Confidential information about safeguarding, behaviour or staff HR records.
- Is it clear what has happened to the data – has it been lost, stolen, accessed, copied, altered or deleted?
- If data has been lost or stolen, were protective measures in place (e.g. encryption, strong passwords)?
- If data has been compromised, have effective measures mitigated the impact (e.g. backed-up copies, pseudonymisation)?
- Has personal data been compromised? If so:
  - Approximately how many individuals are affected?
  - Who are they (pupils, parents/carers, staff, governors, volunteers, suppliers)?
  - Could the information be misused or manipulated (e.g. identity theft, fraud, bullying)?

- Could harm come to individuals, including risks to:
  - Physical safety
  - Emotional wellbeing
  - Reputation

    - Finances
    - Identity
    - Private or sensitive matters becoming public
- Are there wider implications, such as:
    - Loss of public confidence or damage to the school's reputation?
    - Disruption to teaching, learning or operational services?
- Who can help or advise the school (e.g. LA, DPO, ICT provider, ICO, police, insurers)?

13.2 Where those assessing the risk are uncertain, they will seek advice from the DPO (if appointed) and/or the Information Commissioner's Office (ICO).

14. Consideration of further notification

14.1 The school will consider whether there are any legal, contractual or regulatory requirements to notify individuals or organisations affected by, or who have an interest in, the breach.

14.2 The school will consider whether notification will help it meet its obligations under the security principle of UK GDPR (integrity and confidentiality) and the accountability principle.

14.3 The school will assess whether notification could help affected individuals, for example by enabling them to:

- Change passwords.
- Cancel cards or alert their bank.
- Be alert to potential phishing or identity theft.

14.4 Where notification is appropriate, the school will consider:

- Who to notify (e.g. individuals, parents/carers, staff, contractors, LA, insurers, banks, DfE).
- What information to provide, including:
    - A description of how and when the breach occurred.
    - What type of data was involved.
    - What has been done, and will be done, to address the breach and reduce risks.
    - Specific and clear advice on steps individuals can take to protect themselves.
    - Contact details for further questions.
- How to communicate (e.g. letter, email, secure portal, phone call for serious cases).

14.5 The school will consult the ICO guidance on when and how to notify them about breaches.

14.6 The school will consider whether to notify any other third parties who may help or be affected (e.g. police, insurers, professional bodies, funders, IT providers, banks/credit card companies).

14.7 Under UK GDPR, the school will notify the ICO within 72 hours of becoming aware of a personal data breach where it is likely to result in a risk to the rights and freedoms of individuals. If this deadline is not met, reasons will be documented.

14.8 Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the school will notify those affected directly and without undue delay, unless an exemption applies (e.g. data is strongly encrypted and remains unintelligible).

14.9 Where the breach compromises personal information, the notification will include:

- The nature of the personal data breach, including where possible:
- The categories and approximate number of data subjects concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of the school's Data Controller role and/or DPO.
- A description of the likely consequences of the breach.
- A description of the measures taken or proposed to address the breach and mitigate its adverse effects.

15. Evaluation and response

15.1 After each incident, the Data Controller role will:

Establish the root cause(s) of the breach.

Identify any underlying trends or recurring issues.

15.2 The data and business context involved in the breach will be considered (e.g. safeguarding, HR, finance, curriculum).

15.3 The Data Controller role and Headteacher will identify any weak points in existing technical or organisational security measures.

15.4 The Data Controller role and Headteacher will identify any training or awareness gaps.

15.5 The Data Controller role will produce a short lessons-learned report with recommendations. Following approval by the senior leadership team and, where appropriate), the governing body, the school will implement agreed improvements, such as:

- Policy updates.
- Changes to procedures or technical controls.
- Additional training or communication.

16. Monitoring and review

16.1 This policy will be reviewed by the Headteacher, in conjunction with the Data Controller role (and DPO if applicable), at least every two years, or sooner following a significant incident, change in legislation or guidance.

16.2 The Data Controller role is responsible for monitoring the effectiveness of this policy, amending procedures where necessary, and communicating any changes to staff.

Appendix A – Security Breach Incident Form

Name and contact details of the person reporting / discovering the incident:

Role:

Date and time incident discovered:

Date and time incident occurred (if known):

Description of the incident (what happened, how it was detected):

Description of perceived or actual impact:

Systems / data / devices involved (including asset number/device name where relevant):

Location of equipment / data involved:

Immediate actions taken to contain the incident:

Reported to Headteacher (date/time):

Reported to Data Protection Lead / DPO (date/time):

Reported to ICO? (Yes/No/Not required) ICO reference (if applicable):

Outcome / further actions required:

Completed by (name/signature/date):

Appendix B – What to do if you think there has been a Security or Data Breach

BREACH IDENTIFIED OR SUSPECTED

- Personal data sent to the wrong recipient
- Lost or stolen device or paperwork
- Unauthorised access or suspicious activity

↓

IMMEDIATE SAFEGUARDING RISK?

If YES – follow Child Protection procedures immediately, then continue this process.

↓

STOP AND CONTAIN

- Do not delete emails, files or logs
- Do not attempt to fix the issue yourself
- Disconnect device from Wi-Fi if needed

↓

REPORT IMMEDIATELY (SAME DAY)

Inform:

- Headteacher
- Data Protection Lead / Data Controller
- IT Co-ordinator / IT Technician

↓

RECORD DETAILS

- What happened and when
- What data/systems involved
- Who may be affected
- Actions already taken

↓

INVESTIGATION, ICO NOTIFICATION & RESPONSE

School assesses risk, contains breach, notifies ICO within 72 hours if required, and informs affected individuals where appropriate.

↓

REMEMBER: If in doubt – report it.
Early reporting reduces risk.