Parkview and Redwood Primary School Federation

Cyber Security Policy

Policy review dates and changes

Review date	By whom	Summary of changes made	Date ratified by governors/trustees	Date implemented
July 2025	VD	None	July 2025	July 2025

Contents:

Statement of intent

The Parkview and Redwood Primary School Federation is committed to maintaining the confidentiality, integrity and availability of its information and ensuring that the details of the finances, operations and individuals within the schools are only accessible to the appropriate individuals. It is, therefore, important to implement appropriate levels of access, uphold high standards of security, take suitable precautions, and have systems and procedures in place that support this.

The Federation recognises, however, that breaches in security can occur. In schools, most breaches are caused by human error, so the Federation will ensure all staff are aware of how to minimise this risk. In addition, because most information is stored online or on electronic devices that can be vulnerable to cyber-attacks, the Federation will ensure there are procedures in place to prevent attacks occurring. To minimise both risks, it is necessary to have a contingency plan containing a procedure to minimise the potential negative impacts of any security breach, to alert the relevant authorities, and to take steps to help prevent a repeat occurrence.

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Computer Misuse Act 1990
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- National Cyber Security Centre (N.D.) 'Cyber Essentials'
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ESFA (2022) 'Academy trust handbook 2022'
- (DfE) 'Meeting digital and technology standards in schools and colleges'

This policy operates in conjunction with the following school policies:

- Online Safety Policy
- Data Protection Policy
- Disciplinary Policy and Procedure
- Behaviour Policy
- Social Media Policy
- Remote Education Policy
- Cyber Response and Recovery Plan

2. Types of security breach and causes

Unauthorised use without damage to data – involves unauthorised persons accessing data on the school system, e.g. 'hackers', who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it. This includes unauthorised people within the Trust, e.g. schools where pupils access systems that staff have left open and/or logged in, or where staff access data beyond their authorisation, as can occur in schools where all staff are given admin-level access for ease.

Unauthorised removal of data – involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g. a staff member with authorised access who passes the data on to a friend without authorised access. This is also known as data theft. The data may be forwarded or deleted altogether.

Damage to physical systems – involves damage to the hardware in the school's ICT systems, which may result in data being inaccessible to the school and/or becoming accessible to unauthorised persons.

Unauthorised damage to data – involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

Breaches in security may be caused by the actions of individuals, and may be accidental, malicious or the result of negligence:

- Accidental breaches can occur as a result of human error or insufficient training for staff, so they are unaware of the procedures to follow
- Malicious breaches can occur as a result of a hacker wishing to cause damage to the school through accessing and altering, sharing or removing data

Breaches caused by negligence can occur as a result of a staff member knowingly disregarding school policies and procedures or allowing pupils to access data without authorisation and/or supervision.

Breaches in security may also be caused by system issues, which could involve incorrect installation, configuration problems or operational errors:

- The incorrect installation of antivirus software and/or use of outdated software can make the school software more vulnerable to a virus
- Incorrect firewall settings being applied, e.g. unrestricted access to the school network, can allow unauthorised individuals to access the school system
- Operational errors, such as confusion between back-up copies of data, can cause the most recent data to be overwritten

3. Roles and responsibilities

The governing body will be responsible for:

- Ensuring the schools have appropriate cyber-security measures in place
- Ensuring the schools have an appropriate approach to managing data breaches in place
- Supporting the Headteachers and other relevant staff in the delivery of this policy
- Ensuring the Federation meets the relevant cyber-security standards

The schools will be responsible for:

- Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy
- Ensuring appropriate user access procedures are in place
- Responding to alerts for access to inappropriate content in line with the Online Safety Policy
- Organising training for staff members in conjunction with the DPO
- Ensuring a log of cyber-security incidents is maintained

The Headteachers will be responsible for:

- The overall monitoring and management of data security
- Taking responsibility for online safety within the school and promoting online safety measures to parents
- Deciding which strategies are required for managing the risks posed by internet use
- Leading on the school's response to incidents of data security breaches
- Assessing the risks to the school in the event of a cyber-security breach.

- Determining which organisations and individuals need to be notified following a data security breach, and ensuring they are notified

The ICT Support Company be responsible for:

- Maintaining an inventory of all ICT hardware and software currently in use at the schools
- Ensuring any out-of-date software is removed from the school systems
- Implementing effective firewalls to enhance network security and ensuring that these are monitored regularly
- Installing, monitoring and reviewing filtering systems for the school network
- Setting up user privileges in line with recommendations from the headteacher
- Maintaining an up-to-date and secure inventory of all usernames and passwords
- Removing any inactive users from the school system and ensuring that this is always up-to-date
- Performing a back-up of all electronic data held by the school, ensuring detailed records of findings are kept.
- Ensuring all school-owned devices have secure malware protection and are regularly updated
- Recording any alerts for access to inappropriate content and notifying the Headteacher

The School Business Leader will be responsible for:

- Organising training and resources for staff on online safeguarding risks and preventative measures.
- Ensuring the relevant policies and procedures are in place to protect pupils from harm, including the Online Safety Policy
- Monitoring online safety incidents which could result in data breaches and reporting these to the DPO
- Acting as the named point of contact within the school on all online safety issues
- Liaising with relevant members of staff on online safety matters, e.g. the DPO and ICT technician
- Working with the ICT technician after a data security breach to determine where weaknesses lie and improve security measures.
- Monitoring and reviewing the effectiveness of this policy, and communicating any changes to staff members

The DSL Safeguarding Lead will be responsible for:

- Assessing whether there is a safeguarding aspect to any cyber-security incident and considering whether any referrals need to be made.

All staff members will be responsible for:

- Understanding their responsibilities in regard to this policy.
- Undertaking the appropriate training.
- Ensuring they are aware of when new updates become available and how to safely install them.

4. Secure configuration

A register will be kept of all ICT hardware and currently in use at the school, including mobile phones provided by the school. The register will be stored on the school's admin drive and will be audited on an annual basis to ensure it is up-to-date. Any changes to the ICT hardware will be documented on the inventory.

All hardware, software and operating systems will require passwords from individual users. The Federation believes that locking down hardware, such as through the use of strong passwords, is an effective way to prevent access to facilities by unauthorised users.

The Federation will consider referring to the five security controls outlined in the National Cyber Security Centre's (NCSC's) 'Cyber Essentials'. These are:

- **Firewalls** – Firewalls function as a barrier between internal networks and the internet. They will be installed on any device that can access the internet, particularly where staff are using public or otherwise insecure Wi-Fi
- **Secure configuration** – The default configurations on devices and software are often as open as possible to ensure ease of use, but they also provide more access points for unauthorised users. The school will disable or remove any unnecessary functions and change default passwords to reduce the risk of a security breach
- **Access control** – The more people have access to data, the larger the chance of a security breach. The school will ensure that access is given on a 'need-to-know' basis to help protect data. All accounts will be protected with strong passwords
- **Malware protection** – The school will protect itself from malware by installing antivirus and anti-malware software

The ICT Support company will:

- Protect every device with a correctly configured boundary, or software firewall, or a device that performs the same function.
- Protect access to the firewall's administrative interface
- Keep firewall firmware up to date
- Block inbound unauthenticated connections by default
- Document reasons why particular inbound traffic has been permitted through the firewall
- Review reasons why particular inbound traffic has been permitted through the firewall often, change the rules when access is no longer needed
- Enable a software firewall for devices used on untrusted networks, like public wi-fi

All devices will be set up in a way that meets the standards described in the technical requirements.

5. Network security

In line with the UK GDPR, the school's ICT Support company will appropriately test, assess, and evaluate any security measures put in place on a regular basis to ensure these measures remain effective.

The school will employ firewalls in order to prevent unauthorised access to the systems.

The school will undertake an Online Safety Audit and filter test annually.

ICT Support will be aware that security standards may change over time with changing cyber threats.

ICT Support will ensure that the security of every device on its network is reviewed regularly.

To ensure that the network is as secure as possible, the school will:

- Keep a register of all the network devices.
- Avoid leaving network devices in unlocked or unattended locations.
- Remove or disable unused user accounts, including guest and unused administrator accounts
- Immediately change passwords which have been compromised or suspected of compromise

Unlicensed hardware or software will never be used by the school.

6. Malware prevention

The school understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.

ICT Support will ensure that all school devices have secure malware protection and undergo regular malware scans in line with specific requirements. ICT Support will update malware protection regularly to ensure it is up-to-date and can react to changing threats. Malware protection will also be updated in the event of any attacks to the school's hardware and software.

Filtering of websites, will ensure that access to websites with known malware are blocked immediately and reported to ICT Support.

The school will use mail security technology, which will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users. ICT Support will review the mail security technology regularly to ensure it is kept up-to-date and effective.

Staff members are not allowed to download apps on any school-owned device. All apps will be installed by ICT Support.

The school will use anti-malware software that:

- Is set up to scan files upon access, when downloaded, opened, or accessed from a network folder
- Scans web pages as they are accessed
- Prevents access to potentially malicious websites, unless risk-assessed, authorised and documented against a specific business requirement

7. User privileges and passwords

The school understands that controlling what users have access to is important for promoting network security and data protection. User privileges will be differentiated, e.g. pupils will have different access to data and the network than members of staff, whose access will also be role-based.

The Headteacher/School Business Leader will clearly define what users have access to and will communicate this to ICT Support via email. ICT Support will ensure that user accounts are set up to allow users access to the facilities required, in line with the Headteacher/School Business Leader's instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

All users will be required to change their passwords if they become known to other individuals,

The school will implement a user account creation, approval and removal process which is part of the school joining and leaving protocols.

User accounts and access privileges will be appropriately controlled, and only authorised individuals will have an account which enables them to access, alter, disclose or delete personal data.

8. Monitoring usage

Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff. The school will inform all pupils and staff that their usage will be monitored, as well as how it is being monitored and why, in accordance with the school's Online Safety Policy.

If a user accesses inappropriate content or a threat is detected, an alert will be sent to ICT Support.

ICT Support will record any alerts using and will report this to the Headteacher. All incidents will be responded to in accordance with the data breach procedures.

ICT Support will ensure that websites are filtered regularly for inappropriate and malicious content. Any member of staff or pupil that accesses inappropriate or malicious content will be recorded.

All data gathered by monitoring usage will be kept by ICT Support for easy access when required. This data may be used as a method of evidence for supporting a not-yet-discovered breach of network security. In addition, the data may be used to ensure the school is protected and all software is up-to-date.

9. Removable media controls

The school understands staff may need to access the school network from outside the school premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.

ICT Support will encrypt all school-owned devices for, such as laptops and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

When using laptops, tablets and other portable devices, the Headteacher will determine the limitations for access to the network.

ICT Support will use encryption to filter the use of websites on school-owned devices in order to prevent inappropriate use and external threats which may compromise network security when bringing the device back onto the premises. The school uses tracking technology where possible to ensure that lost or stolen school-owned devices can be retrieved.

All data will be held on systems centrally in order to reduce the need for the creation of multiple copies, and/or the need to transfer data using removable media controls.

The Wi-Fi network at the school will be password protected and will only be given out as required. Staff are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless agreed prior to use.

Staff and pupils will adhere to data protection legislation and the school's related policies when working remotely.

Staff will receive annual training regarding what to do if a data protection issue arises from any home working or remote learning.

Wherever possible, personal data will not be taken home by staff members for the purposes of home working, due to the risk of data being lost or the occurrence of a data breach.

Staff and pupils are not permitted to let their family members or friends use any school equipment, in order to protect the confidentiality of any personal data held on the device. Any staff member found to have shared personal data without authorisation will be disciplined in line with the Disciplinary Policy. This may also result in a data breach that the school would need to record and potentially report to the DPO.

Staff will be informed that caution should be exercised while accessing personal data if an unauthorised person is in the same room. If a member of staff needs to leave their device unattended, the device should be locked.

To ensure reasonable precautions are taken when managing data, staff will avoid:

- Sending work emails to and from personal email addresses
- Leaving logged-in devices and files unattended
- Using an unsecured Wi-Fi network

Staff working from home will be encouraged and enabled to go paperless, where possible, as paper files cannot be protected digitally and may be misplaced.

10. Backing up data

ICT Support performs a back-up of all electronic data held by the school daily. This is backed up to the Cloud.

Where possible, back-ups are run overnight and are completed before the beginning of the next working / school day.

11. Avoiding phishing attacks

Staff will use the following warning signs when considering whether a communication may be unusual:

- Is it from overseas?
- Is the spelling, grammar and punctuation poor?
- Is the design and quality what you would expect from a large organisation?
- Is it addressed to a 'valued customer', 'friend' or 'colleague'?
- Does it contain a veiled threat that asks the staff member to act urgently?
- Is it from a senior member of the school asking for a payment?
- Is it from a supplier advising of a change in bank account details for payment?
- Does it sound too good to be true? It is unlikely someone will want to give another individual money or access to another service for free.
- Is it from a generic email address, such as Gmail or Hotmail?

ICT Support will ensure that an appropriate email filtering system is used to identify which emails would be classed as junk or spam, applied in accordance with the 'Malware prevention' section of this policy. ICT Support will ensure that the filtering system is neither too strict nor too lenient, to allow the correct emails to be sent to the relevant folders.

The Headteacher will ensure the school's Social Media Policy includes expectations for sharing of information and determines what is and is not appropriate to share.

The Headteacher will ensure parents, pupils, staff and other members of the school community are aware of acceptable use of social media and the information they share about the school and themselves.

12. User training and awareness

The Headteacher and School Business Leader will arrange training for staff on a regular basis to ensure they are aware of how to use the network appropriately. This will cover identifying irregular methods of communication in order to help staff members spot requests that are out of the ordinary, such as receiving an invoice for a service not used, and who to contact if they notice anything unusual. Unusual communications could come in a variety of forms, e.g. emails, phone calls, text messages or social media messages.

The Headteacher and School Business Leader will arrange for staff to undertake the appropriate training relating to online safety issues.

The Headteacher and School Business Leader will also arrange training for and staff on an annual basis on maintaining data security, preventing data breaches, and how to respond in the event of a data breach.

Through training, all staff will be aware of who they should inform first in the event that they suspect a security breach, and who they should inform if they suspect someone else is using their passwords. All staff will receive training as part of their induction programme.

All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks, in accordance with the process detailed in the Disciplinary Policy and Procedure.

13. Cyber-security incidents

Any individual that discovers a cyber-security incident will report this immediately to the Headteacher.

When an incident is raised, the Headteacher or School Business Leader will inform the DPO of the following information:

- Name of the individual who has raised the incident
- Description and date of the incident
- Description of any perceived impact
- Description and identification codes of any devices involved, e.g. school-owned laptop
- Location of the equipment involved
- Contact details for the individual who discovered the incident
- Whether the incident needs to be reported to the relevant authorities, e.g. the ICO or police

The Headteacher will take the lead in investigating the incident. The DPO, as quickly as reasonably possible, will ascertain the severity of the incident and determine if any personal data is involved or has been compromised. The DPO will oversee a full investigation and produce a report. The cause of the incident, and whether it has been contained, will be identified – ensuring that the possibility of further loss or jeopardising of data is eliminated or restricted as much as possible.

If the DPO determines that the severity of the security breach is low, the incident will be managed in accordance with the following procedures:

- In the event of an internal breach, the incident is recorded using an incident log, and by identifying the user and the website or service they were trying to access
- The Headteacher will issue disciplinary sanctions to the pupil or member of staff who caused the breach, in accordance with the Disciplinary Policy
- In the event of any external or internal breach, the school will record this using an incident log and respond appropriately, e.g. by requesting that there is an update to the firewall, changes to usernames and passwords
- The school will organise updated staff training following a breach
- Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups

Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the DPO will inform the police of the security breach.

Schools are required to report personal data breaches to the DPO if there is a likelihood of risk to people's rights and freedoms. If the DPO decides that risk is unlikely, the breach does not need to be reported; however, the school will need to justify this decision and document the breach.

The DPO will be notified within 72 hours of becoming aware of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

The UK GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours. The information required can be provided in phases, as long as this is done without undue further delay.

In line with the UK GDPR, the following must be provided to the DPO/ICO when reporting a personal data breach:

- A description of the nature of the breach, including, where possible:
  - The categories and approximate number of individuals concerned
  - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the breach
- A description of the measures taken, or proposed to be taken, to deal with the breach
- A description of the measures taken to mitigate any possible adverse effects, where appropriate

ICT Support will test all systems to ensure they are functioning normally, and the incident will only be deemed 'resolved' when it has been assured that the school's systems are safe to use.

14. Assessment of risks

The following questions will be considered by the DPO to fully and effectively assess the risks that the cyber-security breach has brought, and to help take the next appropriate steps. All relevant questions will be clearly and fully answered in the DPO's report, which should record:

- What type of, and how much, data is involved?
- How sensitive is the data? Sensitive data is defined in the UK GDPR; some data is sensitive because of its very personal nature (e.g. health records) while other data types are sensitive because of what might happen if it is misused (e.g. bank account details).
- Is it possible to identify what has happened to the data – has it been lost, stolen, deleted or tampered with?
- If the data has been lost or stolen, were there any protective measures in place to prevent this, such as data and device encryption?
- If the data has been compromised, have there been effective measures in place that have mitigated the impact of this, such as the creation of back-up tapes and spare copies?
- Has individuals' personal data been compromised – how many individuals are affected?
- Who are these individuals – are they pupils, staff, governors, volunteers, stakeholders, suppliers?
- Could their information be misused or manipulated in any way?
- Could harm come to individuals? This could include risks to the following:
    - Physical safety
    - Emotional wellbeing
    - Reputation
    - Finances
    - Identity
    - Private affairs becoming public
- Are there further implications beyond the risks to individuals? Is there a risk of loss of public confidence and/or damage to the school's reputation, or risk to the school's operations?
- Who could help or advise the school on the breach? Could the LA, external partners, authorities, or others provide effective support?
- Does the breach need to be reported to the ICO? If so, has it been successfully reported without undue delay?

15. Consideration of further notification

The DPO will consider whether there are any legal, contractual or regulatory requirements to notify individuals or organisations that may be affected or who will have an interest in data security.

The DPO will assess whether notification could help the individual(s) affected, and whether the individual(s) could act on the information provided to mitigate risks.

The DPO will consider who to notify, what to tell them and how they will communicate the message, which may include:

- A description of how and when the breach occurred and what data was involved.
- Details of what has already been done to respond to the risks posed by the breach.
- Specific and clear advice on the steps they can take to protect themselves, and what the school is willing to do to help them.
- A way in which they can contact the school for further information or to ask questions about what has occurred.

The DPO will consider, as necessary, the need to notify any third parties, such as the police, insurers, professional bodies, funders, trade unions, website and/or system owners, banks and/or credit card companies, who can assist in helping or mitigating the impact on individuals.

16. Evaluation

The school will document all the facts regarding the breach, its effects and the remedial action taken. This should be an evaluation of the breach, and what actions need to be taken forward.

The school will consider the data and contexts involved, establish the root of the breach, and where any present or future risks lie, taking into consideration whether the breach is a result of human or systematic error and see how a recurrence can be prevented.

The Headteacher will identify any weak points in existing security measures and procedures, as well as identifying any weak points in levels of security awareness and training.

The Headteacher will report on findings and implement the recommendations of the report after analysis and discussion.

17. Monitoring and review

This plan will be reviewed by the Federation on an annual basis.

The Headteacher will be responsible for monitoring the effectiveness of this policy, amending necessary procedures and communicating any changes to staff members.