Cyber Security Policy

Responsibility for Document:	Head Teacher
Approved by/date:	Spring 2024
Review:	Spring 2025

Table of Contents

1. Statement of principles

Denmead Junior School 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 school are only accessible to the appropriate individuals. It is 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 school recognises that breaches in security can occur. In schools, most breaches are caused by human error, so the school 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 school 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.

2. 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
- ICO (2021) ‘Guide to the UK General Data Protection Regulation (UK GDPR)’
- (DfE) ‘Meeting digital and technology standards in schools and colleges’

This policy operates in conjunction with the following school policies:

- ICT Acceptable Use Agreement,
- Data Protection policy,
- Code of Conduct,
- Staff Discipline, Conduct and Grievance policy,
- Behaviour Policy,
- E-Safety policy.

3. Types of security breach and causes

Unauthorised use without damage to data

This 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 school, 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

This 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

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

Unauthorised damage to data

This 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 if a staff member knowingly disregards school policies and procedures or allows 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.

4. Roles and responsibilities

Governing Body

The Governing Body will be responsible for:

- Ensuring the school has appropriate cyber-security measures in place.
- Ensuring the school has an appropriate approach to managing data breaches in place.
- Ensuring the school meets the relevant cyber-security standards.

Headteacher

The Headteacher 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.
- Organising training for staff members with the IT Coordinator and DPO.

Data Protection Officer (DPO)

The DPO (Senior Admin Officer) will be responsible for:

- The overall monitoring and management of data security.
- 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, including leading the cyber recovery team.
- Determining which organisations and individuals need to be notified following a data security breach, and ensuring they are notified.
- Working with IT Provider, the IT Coordinator and Headteacher after a data security breach to determine where weaknesses lie and improve security measures.
- Monitoring and reviewing the effectiveness of this policy, alongside the Headteacher, and communicating any changes to staff members.

IT Coordinator / IT Provider

The IT Coordinator/IT Provider will be responsible for:

- Maintaining an inventory of all ICT hardware and software currently in use at the school.
- 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.
- 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.

Designated Safeguarding Lead (DSL)

The DSL 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

All staff members will be responsible for:

- Understanding and carrying out their responsibilities in regard to this policy.
- Undertaking the appropriate training.
- Remaining vigilant to potential risks.

5. Secure configuration

An inventory will be kept of all ICT hardware and software currently in use at the school, provided by the school. This will be audited on a regular basis. Any changes to the ICT hardware or software will be documented using the inventory and will be authorised by the IT Provider before use.

All systems will be audited on a regular basis by the IT Provider. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and will be recorded in the inventory.

Any software that is out-of-date or reaches its ‘end of life’ will be removed from systems.

All hardware, software and operating systems will require passwords from individual users. Passwords will be changed at regular intervals, to prevent access to facilities which could compromise network security.

The school 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 National Cyber Security Centre’s (NCSC’s) ‘Cyber Essentials’ 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, and where necessary, two-factor authorisation.

- **Malware protection** – The school will protect itself from malware by installing antivirus and anti-malware software and using techniques such as whitelisting and sandboxes.

- **Patch management** – The school will install software updates as soon as they are available. If the manufacturer stops offering support for the software, the school will replace it with a more up-to-date alternative.

IT Provider will:

- Protect every device with a correctly configured boundary / software firewall.
- Change the default administrator password or disable remote access on each firewall.
- Protect access to the firewall's administrative interface with multi-factor authentication (MFA), or a small, specified IP-allow list combined with a managed password, or prevent access from the internet entirely.
- Keep firewall firmware up to date.
- Block unauthenticated inbound 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 and 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.

6. Network Security

In line with the UK GDPR, the school will appropriately test, assess, and evaluate any security measures to ensure these measures remain effective.

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

The school’s firewall will be deployed as a centralised deployment through the Broadband Provider, which means the broadband service connects to a firewall that is located within a data centre or other major network location.

As the school’s firewall is managed locally by a third party, the firewall management service will be investigated by the IT Provider to ensure that:

- Any changes and updates that are logged by authorised users within the school are undertaken efficiently by the provider to maintain operational effectiveness.
- Patches and fixes are applied quickly to ensure that the network security is not compromised.

The school is aware that security standards change over time with changing cyber threats. The school 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.
- Change default device passwords.
- Require authentication for users to access sensitive school data or network data.
- Set up filtering and monitoring services to work with the network’s security features enabled.
- Immediately change passwords which have been compromised or suspected of compromise.

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

All unpatched or unsupported hardware or software will be replaced by the IT Provider. Where it is not possible to replace these devices, they will have their access to the internet removed so that scanning tools cannot find weaknesses.

7. 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.

The IT Provider will ensure that all school devices have secure malware protection and undergo regular malware scans in line with specific requirements. Malware protection will also be updated in the event of any attacks on the school’s hardware and software.

Filtering of websites will ensure that access to websites with known malware are blocked immediately and reported to the IT Provider.

The school will use mail security technology, intended to detect and block any malware that is transmitted by email. This also detects spam or other messages which are designed to exploit users.

Staff members are only permitted to download apps on any school-owned device from manufacturer-approved stores and with prior approval from the IT Co-ordinator. Where apps are installed, the IT Provider will keep them up-to-date with any updates, ensuring staff are informed of when updates are ready and how to install them.

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.

8. 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 and Senior Admin Officer will clearly define what users have access to and will communicate this to the IT Provider. The IT Provider will ensure that user accounts are set up to allow users access to the facilities required, in line with the Headteacher's instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

All users will be required to change their passwords on a regular basis and/or if they become known to other individuals, in line with the 'Secure configuration' section of this policy.

Pupils are responsible for remembering their passwords, however, the IT Provider and the IT Co-ordinator will have an up-to-date record of all pupils' usernames and passwords and will be able to reset them if necessary.

Multi-factor authentication (multiple different methods of verifying the user's identity) should be used wherever possible.

The master user account is used as the 'administrator' which allows designated users to make changes that will affect other users' accounts in the school, such as changing security settings, monitoring usage, and installing software and hardware.

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.

9. 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 ICT Acceptable Use Agreement.

If a user accesses inappropriate content or a threat is detected, an alert will be sent to the IT Co-ordinator and Headteacher from the firewall/filtering solution, or to the IT Provider from the anti-virus solution. Alerts will also be sent for unauthorised and accidental access. Alerts will identify the user, the activity that prompted the alert, and the information or service the user was attempting to access.

The Broadband Provider generates a daily report on any alerts in the firewall/filtering, this report is sent to the Headteacher, Assistant Headteacher and IT Co-ordinator. They will inform the DPO as appropriate. All incidents will be responded to in accordance with the 'Data security breach incidents' section of this policy.

The IT Provider and current monitoring service will ensure that websites are filtered on a case-by-case basis for inappropriate and malicious content. Any member of staff or pupil that accesses inappropriate or malicious content will be recorded in accordance with the monitoring process in the 'Data security breach incidents' section of this policy.

The Broadband Provider as the firewall/filtering provider will ensure that websites are filtered as per government requirements for inappropriate and malicious content.

Any alerts from the anti-virus system that are considered a risk will be investigated further by the IT Provider.

All data gathered by monitoring usage will be kept within the school's secure Microsoft 365 system 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.

10. Removable media controls

The school understands that pupils and staff will need to access the school's secure Microsoft 365 system 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.

The IT Provider will encrypt all school-owned devices, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

Before distributing any school-owned devices, the IT Provider will ensure that manufacturers' default passwords have been changed. A set password will be chosen, and the staff member will be prompted to change the password once using the device.

When using laptops, tablets and other portable devices, the Headteacher will determine the limitations for access to the network, as described in the 'Network security' section of this policy.

Staff who use school-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off the school premises.

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.

11. Remote working

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.

Staff and pupils may be required to use their own devices for accessing remote working documents via Microsoft Teams.

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 and Procedure. This may also result in a data breach that the school would need to record and potentially report to the ICO.

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.

Personal data should only be accessed on or transferred to a home device if this is necessary for the member of staff to carry out their role. When sending confidential information, staff must never save confidential information to a personal or household device.

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

- Keeping personal data on unencrypted hard drives.
- Sending work emails to and from personal email addresses.
- Leaving logged-in devices and files unattended.
- Using shared home devices where other household members can access personal data.
- Using an unsecured Wi-Fi network.

The school's procedures for taking data off the school premises will apply to both paper-based and electronic data.

Parents / carers and pupils will be encouraged to contact the DSL or school office if they wish to report any concerns regarding online safety.

Any devices that are used by staff for remote working will be assessed by the IT Provider, using the following checks:

- System security check – the security of the network and information systems.
- Data security check – the security of the data held within the systems.
- Online security check – the security of any online service or system, e.g. the school website.
- Device security check – the security of the personal device, including any 'bring your own device' systems.

If a staff member or pupil decides to leave the school permanently, all data in any form will be returned on or before their last day.

12. Backing up data

The IT Provider performs a back-up of all electronic data held once daily to the cloud, and the date of the back-up is recorded in the backup system. Each back-up is retained for three months locally, then a monthly backup is kept for up to 1 year in the cloud before being deleted.

The IT Provider will ensure that there are at least three backup copies of important data, on at least two separate devices – one of which will remain off-site, e.g. cloud backups.

Local back-ups are run automatically at 11am, 3pm, 9pm and midnight. Cloud backups are run overnight, starting at midnight, and are completed before the beginning of the next school day. Upon completion of back-ups, data is stored on the school's hardware, which is password protected. Data will be replicated and stored in accordance with the school's Data Protection Policy. Only authorised personnel will be able to access back-ups of the school's data.

The school will ensure that offline or 'cold' back-ups are secured. This can be done by only digitally connecting the back-up to live systems when necessary, and never having all offline back-ups connected at the same time.

The school's back-up is automatically tested by the backup solution once a day to ensure that it is viable. It is also manually tested by the IT Provider per visit. All testing will be recorded in the SLA Ticket.

13. Avoiding phishing attacks

The IT Provider will configure all staff accounts using the principle of 'least privilege' – staff members are only provided with as much rights as are required to perform their jobs.

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?

To prevent anyone having access to unnecessary personal information, the DPO will ensure the school's social media accounts and websites are reviewed on a termly basis, making sure that only necessary information is shared.

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.

14. User training and awareness

Annually, the Headteacher will arrange training for staff to ensure they are aware of how to use the network appropriately. They will then train / remind the pupils.

This will cover identifying irregular methods of communication 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.

As well as maintaining data security, preventing data breaches, and how to respond in the event of a data breach, training for all staff members will be arranged by the online safety officer and DPO within a month following an attack, breach or significant update.

Through training, all pupils and staff will be aware of who they should inform first if they suspect a security breach, and who they should inform if they suspect someone else is using their passwords.

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 Behaviour policy and the Staff Discipline, Conduct and Grievance policy.

Cyber-security incidents

All cyber-security incidents will be managed in line with this policy.

Any individual that discovers a cyber security incident will report this immediately to the Headteacher, IT Co-ordinator and the DPO.

When an incident is raised, the DPO will record 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 school's DPO will take the lead in investigating the incident, with assistance from the IT Provider.

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:

- For 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 Behavioural Policy or Disciplinary Policy and Procedure.
- The school will work with the IT Provider to provide an appropriate response to the attack, including any in-house changes.
- 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 the security risk is high, the DPO will establish what steps need to be taken to prevent further data loss, which will require support from various school departments and staff. This action will include:

- Informing relevant staff of their roles and responsibilities in areas of the containment process.
- Taking systems offline.
- Retrieving any lost, stolen or otherwise unaccounted for data.
- Restricting access to systems entirely or to a small group.
- Backing up all existing data and storing it in a safe location.
- Reviewing basic security, including:
  - Changing passwords and login details on electronic equipment.
  - Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.

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 ICO 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 notify the ICO 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 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.

The school will report a personal data breach via the ICO website. The school will also make use of the ICO's self-assessment tool to determine whether reporting a breach is a necessary next step.

Where a breach is likely to result in a significant risk to the rights and freedoms of individuals, the DPO will notify those concerned directly of the breach without undue delay.

Where the school has been subject to online fraud, scams or extortion, the DPO will also report this using the Action Fraud website.

The DPO and the IT Provider 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.

15. 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.

- What type of, and how much, data is involved?
- How sensitive is the data?
- 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 any individual's 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?
- 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?
- Does the breach need to be reported to the ICO? If so, has it been successfully reported without undue delay?

If the DPO, or other people involved in assessing the risks to the school, are not confident in the assessment of risk, they will seek advice from the ICO.

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, e.g. by cancelling a credit card or changing a password. In line with the ‘Data security breach incidents’ section of this policy, if a large number of people are affected, or there are very serious consequences, the ICO will be informed.

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 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.

Evaluation

The DPO will document all the facts regarding the breach, its effects and the remedial action taken.

The DPO 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 DPO, IT Co-ordinator and Headteacher will identify any weak points in existing security measures and procedures. The DPO and IT Co-ordinator will work with the IT Provider to improve security procedures wherever required. The DPO and IT Co-ordinator will identify any weak points in levels of security awareness and training.

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