Walking Tall
Richardson Dees Primary School

Data and Cyber-Security Breach Prevention and Management Plan

Last updated: 17 March 2022

Contents:

Statement of intent

Richardson Dees Primary 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 by the appropriate individuals. It is, therefore, important to uphold high standards of security, take suitable precautions, and to have systems and procedures in place that support this.

The school recognises, however, 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 the risk. In addition, because most information is stored online or on electronic devices which are increasingly 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.

1. Legal framework

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

- The Computer Misuse Act 1990
- The General Data Protection Regulation (UK GDPR)
- Data Protection Act 2019
- National Cyber Security Centre (2018) 'Cyber Security: Small Business Guide'
- National Cyber Security Centre (N.D.) 'Cyber Essentials'
- ICO (2021) 'Guide to the UK General Protection Regulation (UK GDPR)'

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

- Online Safety Policy
- Data Protection Policy
- Acceptable Use Policy
- Disciplinary Policy and Procedure
- Behavioural Policy

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 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 – 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 system, 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 as a result of actions by individuals, which 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 as a result of system issues, which could involve incorrect installation, configuration problems or an operational error:

- 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 DPO is 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.
- Assessing the risks to the school in the event of a data security breach.
- Producing a comprehensive report following a full investigation of a data security breach.
- Determining which organisations and individuals need to be notified following a data security breach, and ensuring they are notified.
- Working with the ICT Technician, School Business Manager and headteacher after a data security breach to determine where weaknesses lie and improve security measures.
- Organising training for staff members on data security, network security and preventing breaches.
- Monitoring the effectiveness of this policy, alongside School Business Manager and headteacher, and communicating any changes to staff members.

The ICT Technician and School Business Manager are responsible for:

- Maintaining an inventory of all ICT hardware and software currently in use at the school.
- Ensuring any software that is out-of-date 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 inventory of all usernames and passwords.
- Removing any inactive users from the school system, ensuring that this is always up-to-date.
- Installing appropriate security software on staff members' personal devices where the headteacher has permitted for them to be used for work purposes.
- Performing a back-up of all electronic data held by the school, ensuring detailed records of findings are kept.
- Recording any alerts for access to inappropriate content and notifying the headteacher.
- Organising training and resources for staff online safeguarding risks and preventative measures.
- Liaising with the LA where appropriate.
- Ensuring relevant policies and procedures are in place to protect pupils from harm, including the Online Safety Policy.

The headteacher is responsible for:

- Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy.
- Defining users' access rights for both staff and pupils, communicating these to the ICT Technician / School Business Manager and maintaining a written record of privileges.
- Responding to alerts for access to inappropriate content in line with the Online Safety Policy.
- Informing the ICT Technician / School Business Manager of staff members who are permitted to use their personal devices for work purposes so that appropriate security methods can be applied.
- Overseeing any necessary disciplinary actions in response to a data security breach.
- Organising training for staff members in conjunction with the School Business Manager and DPO.

All staff members are 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

An inventory will be kept of all ICT hardware and software currently in use at the school, including mobile phones and other personal devices provided by the school. The inventory will be stored online in the School Business Manager's OneDrive and will be audited on an ongoing basis to ensure it is up-to-date. Any changes to the ICT hardware or software will be documented using the inventory and will be authorised by the ICT Technician / School Business Manager before use.

All systems will be audited by the School Business Manager or ICT Technician to ensure the software is up-to-date. 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, e.g. when suppliers end their support for outdated products, meaning that the product is not able to fulfil its purpose anymore.

All hardware, software and operating systems will require passwords from individual users. Passwords will be changed on a regular basis 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 school 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 here 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 (a cyber-security strategy under which a used can only take actions on their computer that an administrator has explicitly allowed in advance) and sandboxes (an isolated virtual machine in which potentially unsafe software code can execute without affecting network resources or local applications).
- **Patch management** – The school will instal software updates as soon as they are available to minimise the time frame in which vulnerabilities can be exploited, If the manufacturer stops offering support for the software, the school will replace it with a more up-to-date alternative.

5. Network security

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

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

Centralised firewall deployment

The school's firewall will be deployed as a centralised deployment, 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 thoroughly investigated by the ICT Technician and School Business Manager 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 will consider installing additional firewalls on the servers in addition to the third-party service as a means of extra network protection. This decision will be made by the School Business Manager, taking into account the level of security currently provided and any incidents that have occurred.

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.

The School Business Manager & ICT Technician will ensure that all school devices have secure malware protection and undergo regular malware scans in line with specific requirements. The School Business Manager & ICT Technician will update malware protection 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, as detailed in 'User privileges and passwords' section of this policy, will ensure that access to websites with known malware are blocked immediately and reported to the School Business Manager & ICT Technician.

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. The School Business Manager & ICT Technician will review the mail security technology ensure it is kept up-to-date and effective.

Staff members are only permitted to download apps on any school-owned device from manufacturer-approved stores and with prior approval from the School Business Manager

& ICT Technician. Where apps are installed, the School Business Manager & ICT Technician will keep up-to-date with any updates, ensuring staff are informed of when updates are ready and how to install them.

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 will clearly define what users have access to and will communicate this to the School Business Manager & ICT Technician, ensuring that a written record is kept. The School Business Manager & ICT Technician 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 School Business Manager and / or ICT technician will have an up-to-date record of all usernames and passwords and will be able to reset them if necessary. The record of all usernames and passwords is encrypted. Only the ICT technician has access to this inventory. Multi-factor authentication (multiple different methods of verifying the user's identity) should be used wherever possible.

The 'master user' password used by the ICT technician will be made available to the headteacher and any other nominated senior leader and will be kept in the School Business Manager Office.

The master user account accessed by the ICT technician, DPO and headteacher is subject to a two-factor authentication for logins. This account requires two different methods to provide identity before logging in: a password and a verification code sent to another school-owned device which must be entered following the password. 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.

A multi-user account may be created for visitors to the school, such as volunteers, and access will be filtered as per the headteacher's instructions. Usernames and passwords for this account will be changed on a regular basis and will be provided as required.

Automated user provisioning systems will be employed in order to automatically delete inactive users or users who have left the school. The ICT technician will manage this provision to ensure that all users that should be deleted are, and that they do not have access to the system.

The ICT technician will review the password system on an annual basis to ensure it is working at the required level.

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 Acceptable Use Policy and Online Safety Policy.

If a user accesses inappropriate content or a threat is detected, an alert will be sent to the ICT technician. 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 ICT technician will record any alerts using an incident log and will report this to the DPO. The DPO will then inform the headteacher and online safety officer as appropriate. All incidents will be responded to in accordance with the 'Data security breach incidents' section of this policy, and as outlined in the Online Safety Policy.

The ICT technician will ensure that websites are filtered 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.

All data gathered by monitoring usage will be kept on a secure shared drive 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 that pupils and 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.

The ICT technician will encrypt all school-owned devices for personal use, such as laptops, USB sticks, mobile phones and tablets, 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 ICT technician 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. The ICT technician will check school-owned devices to detect any unchanged default passwords.

Pupils and staff are not permitted to use their personal devices where the school provides alternatives, such as work laptops, tablets and USB sticks, unless instructed otherwise by the headteacher. If pupils and staff are instructed that they are able to use their personal devices, they will ensure that they have an appropriate level of security and firewall to prevent any compromise of the school's network security. This will be checked by the ICT technician.

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. Staff will avoid connecting to unknown Wi-Fi hotspots, such as in coffee shops, when using any school-owned laptops, tablets or other devices, or when accessing school networks.

The online safety officer 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. Pupils are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless agreed prior to usage. A separate Wi-Fi network will be established for pupils and visitors at the school to limit their access to school networks and any other applications which it is not necessary for them to access.

10. Home working and remote learning

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

Staff will receive 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 may be required to use their own devices for the duration of the remote working or learning period. Any user on a personal device will need to access the school system through a proxy, e.g. VPN. Using a shared personal or household device for school purposes should be avoided where possible; however, the school understands that this may not always be possible.

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 who require access to personal data to enable them to work from home will first seek approval from the headteacher, and it will be ensured that the appropriate security

measures are in place by the ICT technician and the DPO, e.g. secure passwords and anti-virus software.

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. School devices will automatically lock after a period of inactivity to avoid an unauthorised person gaining access to the device. Where staff are using a personal device, they will be advised that a similar function should be implemented.

Personal data should only be 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. Data that is transferred from a work to a home device will be encrypted so that if any data is lost, stolen or subject to unauthorised access, it will remain safe until it can be recovered.

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.

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. If sensitive data is taken off the school premises to allow staff to work from home, it will be transported in a lockable bag or container. The school's procedures for taking data off the school premises will apply to both paper-based and electronic data.

When taking physical copies of data, e.g. paper documents and school-owned devices, off the school premises, staff will sign out the documents at the school office. The physical data will be signed back in when staff return it.

Pupils are not permitted to use school-owned devices or software for activities that do not pertain to their online education, e.g. use of social media, gaming, streaming or viewing content that is not applicable to their curriculum. Pupils are not permitted to download any software onto school devices, unless instructed to and approved by their teacher.

Pupils will not alter the passwords or encryptions protecting school documents and systems put in place by the school. Pupils will not alter or disable any security measures that are installed on school devices, e.g. firewalls, malware prevention or anti-virus software. Pupils will not share any confidential and/or personal information made accessible to them, e.g. VPN passwords, with anyone who is not authorised to view that information.

Pupils that do not use school devices or software in accordance with this policy will be disciplined in line with the Behavioural Policy.

Pupils must report any technical issues to their teacher as soon as possible. Parents and pupils will be encouraged to contact the online safety officer if they wish to report any concerns regarding online safety.

Any devices that are used by staff and pupils for remote working and learning will be assessed by the ICT technician prior to being taken to the home setting, 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

The ICT technician will provide staff and pupils with details and instructions for accessing the school network that they will be using throughout the duration of the remote working and learning period.

In the event that 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.

11. Backing-up data

The ICT technician performs a back-up of all electronic data held by the school on a termly basis, and the date of the back-up is recorded using a log. Each back-up is retained for three months before being deleted. The ICT technician performs an incremental back-up monthly of any data that has changed since the previous back-up. The ICT technician will record the date of any incremental back-up, alongside a list of the files that have been included in the back-up.

The school must follow the NCSC's guidance on backing up data where necessary, including:

- Identifying what essential data needs to be backed up.
- Storing backed-up data in a separate location to the original data.
- Consider using the Cloud to store backed-up data.
- Refer to the NCSC's Cloud Security Guidance.
- Ensure that backing up data is regularly practised.

Where possible, back-ups are run overnight 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 Cloud Computing 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.

12. Avoiding phishing attacks

The ICT technician 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.

Designated individuals who have access to the master user account will avoid browsing the web or checking emails whilst using this account. Two-factor authentication is used on any important accounts, such as the master user account, or any key accounts, such as the headteacher's or SBM's accounts.

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?

The ICT technician 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. The ICT technician 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.

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 regular basis, making sure that only necessary information is shared. The headteacher and DPO 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, in accordance with the school's Acceptable Use Policy.

13. User training and awareness

The School Business Manager and headteacher will arrange training for pupils and staff to ensure they are aware of how to use the network appropriately in accordance with the Acceptable Use Policy and E-safety Policy.

The DPO will also arrange training for pupils and staff on 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 School Business Manager and DPO within two weeks following an attack, breach or significant update.

Through training, all pupils and 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, as well as any new pupils who join the school.

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 E-safety Policy.

14. Data security breach incidents

Any individual that discovers a data security breach will report this immediately to the headteacher 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 breach and will be allocated the appropriate time and resources to conduct this. The DPO, as quickly as reasonably possible, will ascertain the severity of the breach and determine if any personal data is involved or has been compromised. The DPO will oversee a full investigation and produce a comprehensive report. The cause of the breach, 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 Behavioural Policy or Disciplinary Policy and Procedure
- The school will work with the third-party 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 ICT technician 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 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?

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

16. Consideration of further notification

The School Business Manager and / or 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 security (see 15.8 onwards for specific GDPR requirements about personal data).

The School Business Manager and / or DPO will assess whether notification could help the individual(s) affected, and whether individuals could act on the information provided to mitigate risks, e.g. by cancelling a credit card or changing a password.

If a large number of people are affected, or there are very serious consequences, the ICO will be informed.

The School Business Manager and / or 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 will be included.
- 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 ICO will be consulted for guidance on when and how to notify them about breaches.

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

The School Business Manager and / or DPO will notify the ICO within 72 hours of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

Where a breach is likely to result in a significant risk to the rights and freedoms of individuals, the School Business Manager and / or DPO will notify those concerned directly of the breach.

Where the breach compromises personal information, the notification will contain:

- The nature of the personal data breach including, where possible:

- The type(s), e.g. staff, pupils or governors, and approximate number of individuals concerned.
- The type(s) and approximate number of personal data records concerned.

- The name and contact details of the School Business Manager and / or DPO or other person(s) responsible for handling the school's information.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed, to deal with and contain the breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

17. Evaluation and response

The School Business Manager and / or DPO will establish the root of the breach, and where any present or future risks lie.

The School Business Manager and / or DPO will consider the data and contexts involved.

The School Business Manager and / or DPO and headteacher will identify any weak points in existing security measures and procedures.

The School Business Manager and / or DPO will work with the ICT Technician to improve security procedures wherever required.

The School Business Manager and / or DPO and headteacher will identify any weak points in levels of security awareness and training.

The School Business Manager and / or DPO will report on findings and, with the approval of the school leadership team, implement the recommendations of the report after analysis and discussion.

18. Monitoring and review

This policy will be reviewed by the headteacher, in conjunction with the School Business Manager and / or DPO and ICT Technician, on an annual basis. The next scheduled review date for this policy is March 2023.

The School Business Manager and / or DPO is responsible for monitoring the effectiveness of this policy, amending necessary procedures and communicating any changes to staff members.