Berkswich CE Primary School			
Reference Number S3e	**Shared with Staff** April 2022	**Ratified by Governing Board** April 2022	**Review Date** April 2024
Policy Title	**Data and E-Security Breach Prevention and Management Plan**		

Contents:

Statement of intent

As a Church of England School, the protection of all within our care is of the utmost importance, as all who step through our doors are loved and cherished as a child of God.

Berkswich CE is committed to maintaining the confidentiality 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, particularly as most information is stored online or on electronic devices which are increasingly vulnerable to cyber-attacks. This being the case, 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

1.1. 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 (GDPR)
- National Cyber Security Centre (2018) 'Cyber Security: Small Business Guide'

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

- E-safety Policy
- Data Protection Policy
- Acceptable Use Policy
- Mobile phone, camera and media device policy
- Staff code of conduct

2. Types of security breach and causes

2.1. **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.

2.2. **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.

2.3. **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.

2.4. **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.

2.5. Breaches in security may be caused as a result of actions by individuals, which may be accidental, malicious or the result of negligence – these can include:

- Accidental breaches, e.g. as a result of insufficient training for staff, so they are unaware of the procedures to follow.
- Malicious breaches, e.g. as a result of a hacker wishing to cause damage to the school through accessing and altering, sharing or removing data.
- Negligence, e.g. as a result of an employee who is aware of school policies and procedures, but disregards these.

2.6. Breaches in security may also be caused as a result of system issues, which could involve incorrect installation, configuration problems or an operational error – these can include:

- Incorrect installation of anti-virus software and/or use of software which is not the most up-to-date version, meaning the school software is more vulnerable to a virus
- Incorrect firewall settings are applied, e.g. access to the school network, meaning individuals other than those required could access the system
- Confusion between backup copies of data, meaning the most recent data could be overwritten

3. Roles and responsibilities

3.1. The data protection officer (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, and for keeping the school's network services, data and users safe, in conjunction with the computing lead.
- 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 computing lead and headteacher after a data security breach to determine where weaknesses lie and improve security measures.
- Organising training for staff members on data security and preventing breaches.
- Monitoring the effectiveness of this policy, alongside the computing lead and headteacher, and communicating any changes to staff members.

3.2. The computing lead is responsible for:

- Maintaining an inventory of all computing and digital hardware and software currently in use at the school.
- Ensuring any software that is out-of-date is removed from the school premises.
- Liaising with the school's technician in implementing effective firewalls to enhance network security and ensuring that these are monitored regularly.
- Liaising with the school's technician in ensuring all school-owned devices have secure malware protection and that devices are regularly updated.
- Liaising with the school's technician in installing filtering systems for the school's network.
- Monitoring and reviewing filtering systems for the school's network.
- Setting up user privileges in line with recommendations from the headteacher.
- Removing any inactive users from the school's system, ensuring that this is always up-to-date.
- Recording any alerts for access to inappropriate content and notifying the headteacher.
- 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.
- Organising training for staff members on network security

.

3.3. 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 computing lead,
- Responding to alerts for access to inappropriate content in line with the E-safety Policy.
- Informing the computing lead of staff members who are permitted to use their personal devices for work purposes so that appropriate security methods can be applied.
- Issuing appropriate disciplinary sanctions to pupils or members of staff who cause a data security breach.
- Organising training for staff members in conjunction with the computing lead and DPO.

4. Secure configuration

4.1. 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. This will be stored on the school network and will be audited on a termly basis by the computing lead to ensure that it is up-to-date.

4.2. Any changes to the ICT hardware or software will be documented using the inventory and will be authorised by the computing lead before use.

4.3. All systems will be audited on a termly basis by the computing lead 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.

4.4. Any software that is out-of-date or reaches its 'end of life' will be removed from systems, i.e., when suppliers end their support for outdated products such that any security issues will not be rectified.

4.5. All hardware, software and operating systems will require passwords from individual users before use. Passwords will be changed on a six monthly basis to prevent access to facilities which could compromise network security.

4.6. 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.

5. Network security

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

5.2. The school's firewall will be deployed as a:

- Centralised deployment: the broadband service connects to a firewall that is located within a data centre or other major network location.
- The school's firewall is part of the Entrust Broadband and maintained by Entrust.

5.3. As the school's firewall is managed locally by a third party, the firewall management service will be thoroughly investigated by the computing lead to ensure that:

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

6. Malware prevention

6.1. 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.

6.2. The computing lead will ensure that all school devices have secure malware protection.

6.3. The school's anti-virus software, Symantec Endpoint, scans for malware and updates itself daily.

6.4. Malware protection will also be updated in the event of any attacks to the school's hardware and software.

6.5. Filtering of websites, as detailed in section 7 of this policy, will ensure that access to websites with known malware are blocked immediately and reported to the computing lead and the technician. .

6.6. The school uses Microsoft365 for email; Microsoft provide filters that block spam. If needed, the school can adjust the filter using the Office365 administrator portal. Any changes are carried out by the technician with the authorisation of the computing lead.

6.7. The computing lead will review the mail security technology on a termly basis to ensure it is kept up-to-date and effective.

6.8. Staff members are only permitted to download apps on any school-owned device from manufacturer-approved stores and with prior approval from the computing lead.

6.9. Where apps are installed, the computing lead will keep up-to-date with any updates, ensuring staff are informed of when updates are ready, how to install them, and that they should do this without delay.

7. User privileges

7.1. The school understands that controlling what users have access to is important for promoting network security. User privileges will be differentiated, i.e. pupils will have different access to data and the network than members of staff.

7.2. The headteacher will clearly define what users have access to and will communicate this to the computing lead, ensuring that a written record is kept.

7.3. The computing lead 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.

7.4. The deputy head will ensure that screen and key captures are reviewed on a weekly basis for inappropriate and malicious content. Any member of staff or pupil who has accessed inappropriate or malicious content will be recorded in accordance with the monitoring process in section 13 of this policy. The headteacher will subsequently act in accordance with school policies related to staff conduct.

7.5. All users will be required to change their passwords on a six monthly basis and will use upper and lowercase letters, as well as numbers and a special character, to ensure that passwords are strong.

7.6. Users will also be required to change their password if they become known to other individuals.

7.7. Pupils are responsible for remembering their passwords; however, the class teacher will keep a secure copy and the technician or relevant member of staff will be able to reset them if necessary (i.e. the English lead will be responsible for sites/apps related to English rather than the technician or class teacher).

7.8. Bitlocker recovery keys for staff encrypted, password protected devices are kept in folders where only the named individual has access privileges.

7.9. All the pupils have their own accounts, with the exception of Nursery. There are class logins for Nursery and Reception. The computer technician will set up their individual user accounts, ensuring appropriate access and that their username and password is recorded in a password protected file by the technician; class teachers can access these if children forget their login details..

7.10. Any 'master user' passwords used by the school's technician will be made available to the headteacher, DPO and any other nominated senior leader.

7.11. 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 use, and installing software and hardware.

7.12. A multi-user 'Guest' account will be created for visitors to the school, such as volunteers or those delivering training, and access will be filtered as per the headteacher's instructions. Usernames and passwords for this account will be changed on an annual basis and will be provided as required.

7.13. There are three supply teacher accounts; usernames and passwords for this account will be changed on an annual basis if used.

7.14. The technician will delete inactive users or users who have left the school. The computing lead will manage this provision to ensure that all users who should be deleted are, and that they do not have access to the system.

7.15. The computer lead is responsible for ensuring that the relevant member of staff has deleted any user accounts, including on apps, they school system and online sites used by the school,S for those who have left the school so that they cannot access the system after leaving.

7.16. The computing lead will review the system on a termly basis to ensure the system is working at the required level.

8. Monitoring usage

8.1. Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff.

8.2. The school will inform all pupils and staff that their usage will be monitored Smoothwall Monitor (supplied by Entrust for computers and iPads) in accordance with the school's Acceptable Use Policy and Online Safety and Digital Devices Policy.

8.3. If a user accesses inappropriate content or a threat is detected, the headteacher and the deputy head are able to identify this through reports generated by the system.

8.4. Records will identify: the user, the computer used, the activity that prompted the alert and the information or service the user was attempting to access.

8.5. The deputy head lead will retain a weekly summary sheet which is co-signed by the headteacher. All incidents will be responded to in accordance with section 13 of this policy, and as outlined in the Online Safety and Digital Devices Policy.

8.6. All data gathered by monitoring usage will be kept in a filing cabinet in the school office for easy access when required. The data may be used to ensure the school is protected and all software is up-to-date.

9. Removable media controls and home working

9.1. Staff do not have access to the school network from areas other than on the premises.

9.2. The computing lead 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.

9.3. Before distributing any school-owned devices, the computing lead will ensure that manufactures' default passwords have been changed. A password will be chosen by the staff member; a recovery key will be kept in a file that can only be accessed by the same user.

9.4. 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.

9.5. 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 computing lead.

9.6. When using laptops, tablets and other portable devices, the headteacher will determine the limitations for access to the network, as described in section 5 of this policy.

9.7. 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.

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

9.9. Any laptop that goes off site has BitLocker enabled to encrypt any files held.

9.10. Where possible, 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.

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

9.12. Visitors to the school will not be given access to the school wifi, unless instructed otherwise by the headteacher.

10. Backing-up data

10.1. The office clerk performs a back-up of all electronic data held by the school on a weekly basis; back up tapes are rotated and kept securely in the office.

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

10.3. Upon completion of back-ups, the back-up is saved onsite on the school's tapes; the data is encrypted.

10.4. Only authorised personnel are able to access the school's data.

11. Avoiding phishing attacks

11.1. The 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.

11.2. Designated individuals who have access to the master user account will avoid browsing the web or checking emails whilst using this account.

11.3. In accordance with section 12 of this policy, the computing lead and headteacher will organise regular training for staff members – this will cover identifying irregular emails 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.

11.4. The headteacher and computing lead will notify staff when other schools or agencies make them aware of phishing attacks on other schools.

11.5. Staff will use the following warning signs when considering whether an email may be unusual:

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

11.6. The computing lead will ensure that email filtering systems, applied in accordance with section 6 of this policy, are neither too strict or lenient; filtering that is too strict may lead to legitimate emails becoming lost, and too lenient

filters may mean that emails that are spam or junk are not sent to the relevant folder.

11.7. To prevent hackers having access to unnecessary public information, the headteacher and 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.

11.8. The headteacher and DPO will ensure the school's policies related to data and use of digital technologies includes expectations for sharing of information – and determines what is and is not necessary to share.

11.9. 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.

12. User training and awareness

12.1. The computing lead and headteacher will arrange training for pupils and staff on a termly basis to ensure they are aware of how to use the network appropriately in accordance with the Acceptable Use Policy and E-safety Policy.

12.2. The headteaacher will also arrange training for pupils and staff on a termly basis maintaining data security, preventing data breaches, and how to respond in the event of a data breach.

12.3. Training for all staff members will be arranged by the computing lead and deputy head within two weeks following an attack, breach or significant update.

12.4. 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.

12.5. All staff will receive training as part of their induction programme, as well as any new pupils who join the school.

12.6. All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks, in accordance with school policies.

13. Security breach incidents

13.1. Any individual who discovers a security data breach will report this immediately to the headteacher and the DPO. Either the DPO or the headteacher will inform the computing lead.

13.2. 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

13.3. The headteacher will take the lead in investigating the breach and will be allocated the appropriate time and resources to conduct this.

13.4. The headteacher, as quickly as reasonably possible, will ascertain the severity of the breach and determine if any personal data is involved or has been compromised.

13.5. The headteacher will oversee a full investigation and produce a report.

13.6. The cause of the breach, and whether or not it has been contained, will be identified – ensuring that the possibility of further loss/jeopardising of data is eliminated or restricted as much as possible.

13.7. 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
- The headteacher will issue disciplinary sanctions to the pupil or member of staff, in accordance with the processes outlined in school policies
- In the event of any external or internal breach, the DPO will record this using an incident log and respond appropriately, e.g. by changing usernames and passwords, updating filtered websites or creating further back-ups of information.

13.8. 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.

13.9. Where the security risk is high, the DPO will establish which 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.
- Altering procedures to ensure that robust systems avoid a similar breach.

13.10. 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.

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

13.12. The 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.

14. Assessment of risks

14.1. The following questions will be considered by the DPO or headteacher 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 breach report and records:

- What type and how much data is involved?
- How sensitive is the data? Sensitive data is defined in the 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/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 Local Authority, external partners, or others provide effective support?

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

15. Consideration of further notification

15.1. 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 security (see 15.8 onwards for specific GDPR requirements about personal data).

15.2. The 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.

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

15.4. 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 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.

15.5. The ICO will be consulted for guidance on when and how to notify them about breaches.

15.6. The 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.

15.7. The 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.

15.8. 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.

15.9. 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 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.

16. Evaluation and response

16.1. The DPO will establish the root of the breach, and where any present or future risks lie.

16.2. The DPO will consider the data and contexts involved.

16.3. The DPO and headteacher will identify any weak points in existing security measures and procedures.

16.4. The DPO will work with the computing lead and the technician to improve security procedures wherever required.

16.5. The DPO and headteacher will identify any weak points in levels of security awareness and training.

16.6. The DPO will report on findings and, with the approval of the school leadership team, implement the recommendations of the report after analysis and discussion.

17. Monitoring and review

17.1. This policy will be reviewed by the headteacher, in conjunction with the DPO and computing lead.

17.2. The DPO is responsible for monitoring the effectiveness of this policy, amending necessary procedures and communicating any changes to staff members.

Timeline of Incident Management – Berkswich CE Primary

Date/time and type of breach	Description of incident, including how the incident was reported and who is responsible for investigating the breach	Potential consequence/s	Action Log (including preventative actions, necessary training or change in school policy or procedure)	Date actions taken and name of person responsible	Reviewed by a representative of the governing board