

**BISHOP HOGARTH CATHOLIC EDUCATION TRUST**

**INFORMATION SECURITY POLICY**

**Document Management:**

Date Policy Approved: 29 April 2015

Date Amended: January 2025

Next Review Date: January 2028

Version: 5.0

Approving Body: Finance & Resources Committee

|  |  |
| --- | --- |
| **Change Log** | |
| **Update:** | **Updated to reflect new requirements for cyber security including planning, risk mitigation and response requirements. Includes the requirement for:**   * **having offline backups and testing regularly** * **making sure all employees Governors and Directors who have access to the school’s information technology system undertake NCSC Cyber Security Training annually** * **registering with Police CyberAlarm** * **having a Cyber Response Plan in place** |
| **Location:** | **Throughout** |
| **Summary Date:** | **30/01/2025** |
| **Completed by:** | **Director of Governance – Julian Kenshole** |

**Information Security Policy**

**[Amended] 1. Legal and Policy Framework**

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

* Computer Misuse Act 1990
* The UK General Data Protection Regulation (UK GDPR)
* Data Protection Act 2018
* National Cyber Security Centre (2018) ‘Small Business Guide: Cyber Security’
* National Cyber Security Centre (NCSC) ‘Cyber Essentials’
* ICO [UK GDPR Guidance and Resources](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/)
* ESFA ‘Academy Trust handbook’
* (DfE) (2023) ‘Meeting digital and technology standards in schools and colleges’

This policy provides a Policy Statement on Information Security and an accompanying set of guidelines for all Trust staff. It is part of a suite of policies and should be read in conjunction with the following:

* Data Protection Policy
* Acceptable Use Policy
* Media Relations Policy
* E Mail Policy
* **[New]** Online Safety Policy
* **[New]** Remote Education Policy
* **[New]** Cyber Security Response Plan
* **[New]** Bring Your Own Device Policy
* **[New]** Home School Agreements

**[Amended] 2. Policy Statement**

The Trust 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. We will therefore implement appropriate levels of access, uphold high standards of security, take suitable precautions, and have systems and procedures in place that support this.

The Trust recognises, nevertheless, that breaches in security can occur, with most breaches caused by human error. We will therefore ensure all staff are aware of how to minimise this risk. Additionally, because most information is stored online or on electronic devices that can be vulnerable to cyber-attacks, we will ensure there are procedures to prevent attacks occurring. To minimise risks, we will adopt Business Continuity and Cyber Security Response Plans 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.

**[Amended] 3. Roles and responsibilities**

**[Amended] The Data Protection Officer is responsible for:**

* Leading on the school’s /Trust’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 IT Directorafter a data security breach to determine where weaknesses lie and improve security measures.
* Organising training for staff members on data and cybersecurity and preventing breaches.
* Monitoring and reviewing the effectiveness of this policy.

**[Amended] The IT Director is responsible for:**

* **[Amended]** The overall monitoring and management of data, network and cyber security.
* **[New]** Regularly update/ refresh the Cyber Essentials Readiness Toolkit and associated action Plan
* **[New]** Seek certification and re-certification through the National Cyber Security Centre’s (NCSC’s) Cyber Essentials.
* **[New]** Producing, regularly reviewing and testing the Cyber Security Response Plan.
* **[New]** Register with Police CyberAlarm
* Deciding which strategies are required for managing the risks posed by internet use.
* Maintaining an inventory of all ICT hardware and software currently in use.
* Ensuring any out-of-date software is removed from Trust and school systems.
* Implementing effective firewalls to enhance network security and ensuring that these are monitored regularly.
* Installing, monitoring and reviewing filtering systems for the Trust network.
* Setting up user privileges in line with recommendations from the headteacher and Data Protection Officer.
* Maintaining an up-to-date and secure inventory of all usernames and passwords.
* Removing any inactive users from the system and ensuring that this is always up-to-date.
* Performing a back-up of all electronic data held by the Trust.
* Ensuring all school-owned devices have secure malware protection and are regularly updated.
* Recording any alerts for access to inappropriate content and notifying relevant staff.

**[Amended] The headteacher is responsible for:**

* [New] The day to day management information security within their school.
* Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy.
* Requesting new user profiles and defining users’ access rights for both staff and pupils for key systems
* Informing the IT Department 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.

**All staff members are responsible for:**

* Understanding their responsibilities in regard to this policy.
* Undertaking the appropriate training.

**4. Security and care of equipment**

All items of equipment are the property of the Trust and as such must be kept well-maintained and secure at all times.

If a member of staff wishes to borrow a piece of equipment, (a laptop, for example) full details will be recorded by the ICT Team or Administrative Staff.

If the equipment is lost or stolen then the Headteacher and the Police must be notified. If the equipment was being used for processing personal data then the procedures given below (Security of data) should have been followed to ensure the data was kept safe from disclosure.

All equipment should be proprietorially marked using an approved security marker to aid identification if recovered, following theft or loss. An asset register which lists all equipment should be kept by the School Business Manager – this should include a list of identifying information such as equipment ID’s.

**[Amended] 4. Security of data**

The Trust has a statutory duty under the Data Protection Act to ensure appropriate organisational technical and organisational measures are taken to protect personal data against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, personal data – see **Appendix 1**.

**[New]** The school will refer to the five security controls outlined in the National Cyber Security Centre’s (NCSC’s) ‘[Cyber Essentials](https://www.ncsc.gov.uk/cyberessentials/overview)’. These are:

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

All staff should ensure that any electronic or paper documents which contain personal data or, are otherwise confidential, are protected against unauthorised access. This includes ensuring that paper records are securely locked away, not just at the end of the day but when staff are out of the office, and that when staff are away from a computer it is switched off, or locked against access and password protected.

Where computers hold personal or confidential data they should be password protected. Any memory sticks or removable devices used to store personal data, or used by staff away from Trust premises, should be password protected and if possible encrypted. Staff should not use their own personal memory sticks or removable devices for work purposes and **MUST NOT** use private equipment to store personal data.

The primary copy of Trust information should never be stored at home, so school records should be updated as soon as possible with copies of any work that staff do at home, and the home copy deleted.

Staff must also take reasonable security measures to protect the information they take home from unauthorised loss, access or amendment. Whenever possible, staff should ensure that copies of school information are not stored on their private PC, including in temporary directories.

When taking paperwork home, staff should ensure that it is stored securely when not in use and is not vulnerable to theft, or accidental access by family members.

Information in transit should be protected by being locked in a briefcase or car boot. Memory sticks and similar are easily lost or mislaid and should be carried securely (not in a pocket or on a lanyard). Memory sticks **must only** be used with the permission of the CEO. Staff should avoid transferring information or equipment from a car interior to a car boot in a car park where the car will subsequently be left, or leaving information or equipment in a car or car boot at any time when the car is unattended.

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.

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.
* Accessing personal data if an unauthorised person is in the same room.

Servers and back-up systems should be kept securely in locked cabinets or a locked area to which only staff have access. Similarly, hardware such as laptops which are kept at the school should be locked away at the end of the day, not left on desks or visible through windows.

Use of emails, scanners or fax systems to transfer data should be limited according to the sensitivity of the data being transferred. Staff must always check that information is being sent to the appropriate recipient. It is strongly suggested that to send sensitive personal data staff use recorded delivery mail which can be tracked or delivered by hand if encryption facilities are not available.

Network security will be maintained through the employment of firewalls to prevent unauthorised access to the system.

**[Amended]** Any software that is out-of-date or reaches its ‘end of life’ will be reviewed and removed from systems where necessary following a risk-based assessment, e.g. when suppliers end their support for outdated products, meaning that the product is not able to fulfil its purpose anymore. Unlicenced hardware or software will never be used by the school.

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. We continually review password security processes.

Staff should not share or give out passwords and should not permit anyone without clearance to access secure information.

The Computer Misuse Act makes it an offence to access any computer system for which access authorisation has not been given. Thus, any attempt to interfere with or try to bypass the security controls on a computing system is an offence. Similarly trying to obtain information, such as users’ passwords or accessing or modifying files belonging to other people who have not given access authorisation is also an offence.

The Trust 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 IT Department will encrypt all Trust-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 IT Department will ensure that manufacturers’ default passwords have been changed.

The Trust automatically backs up data to both remote off-line and on-line environments.

The Trust will seek certification through the National Cyber Security Centre’s (NCSC’s) Cyber Essentials.

**[Amended] 5. Malware prevention**

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

**[New]** Staff will follow procedures for filtering and monitoring to keep pupils safe as set out in the Online Safety Policy. The school’s filtering provider will be:

* A member of [Internet Watch Foundation](https://www.iwf.org.uk/membership/our-members) (IWF)
* Signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
* Effective at blocking access to illegal content

**[New]** The filtering system will be able to identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them, and provide alerts when any web content has been blocked

**[Amended]** Filtering of websites, as detailed in the [user privileges and passwords](#_User_privileges) section of this policy, will ensure that access to websites with known malware are blocked immediately and reported to the IT Department. The Trust ensures the school’s IT network has appropriate filters and monitoring systems in place and that it is meeting the DfE’s ‘[Filtering and monitoring standards for schools and colleges](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges)’.

The Trust uses 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 IT Director will review the mail security technology on a regularbasis to ensure it is kept up-to-date and effective.

Staff members are **not permitted** to download apps on any Trust-owned device. Where apps are installed, the IT Director will keep up-to-date with any updates, ensuring they are installed.

**[Amended] 6. User privileges and passwords**

The Trust 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.

**[New]** The Trust will implement multi-factor authentication for staff and pupils.

All users will be required to change their passwords on a regular basis and/or if they become known to other individuals.

Pupils are responsible for remembering their passwords the IT Department will be able to reset them if necessary.

A multi-user account will be created for visitors to the school, such as volunteers. Usernames and passwords for this account will be changed on a regularbasis (we need to define this) 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 IT Department will manage this provision to ensure that all users that should be deleted are, and that they do not have access to the system.

**[New]** Password strength will be enforced at a system level – the school will use a deny list for automatic blocking of common passwords and passwords must contain a minimum of eight characters.

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

**[New]** 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. Users will have a separate account for routine business if their main account:

* Is an administrative account.
* Enables the execution of software that makes significant system or security changes.
* Can make changes to the operating system.
* Can create new accounts.
* Can change the privileges of existing accounts.

**[New] 7.** **Backing up data**

The Trust will 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.
* Considering using cloud solutions to store backed-up data.
* Referring to the NCSC’s Cloud Security Guidance.
* Ensuring that backing up data is regularly practised.

The school will keep under review where servers can be replaced with cloud solutions, including accessing files, documents and shared folders. Where cloud solutions are used, the school will confirm its ICT provider ensures that data is portable and allows for:

* Secure encrypted transfer.
* Data export to an open standard or commonly used format.
* Data links through secure, documented application programming interfaces (APIs).
* A timely process for data transfer in an open standard or neutral format if the school ends the contract.
* Easy and secure access from a range of devices.

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 Trust’s hardware, which is password protected. Only authorised personnel will be able to access back-ups of the Trust’s data. Backup is undertaken daily.

The Trust 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 Trust’s back-up strategy will be tested on a regular basis. All testing will be recorded.

**[Amended] 8. Avoiding phishing attacks**

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

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

The IT Director will ensure that an appropriate email filtering system is used to identify which emails would be classed as junk or spam. The IT Director 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 Headteacher will ensure the school’s social media account passwords and websites are held securely. The Schools will not create social media accounts without first seeking the authority of CEO /DCEO.

**[New]** The Trust will develop guidance on what information should not be shared via social media sites.

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 Trust’s Acceptable Use Policy and Home-School Agreements.

**9. Secure Disposal**

All confidential waste paper should be shredded and / or disposed of through a confidential waste service. This includes personal data due for destruction, duplicates of personal data and other confidential information.

Computer systems must be fully cleansed of any information before they are disposed of or re-sold. Approval and support for this must be obtained from the IT Director. Discs, memory sticks and other removable devices should be destroyed if they are intended for disposal.

**10. Security of buildings**

All staff must wear ID badges. Staff should be prepared to challenge any member of the public within the school to ensure that they have a right to be there.

Any contractor should carry identification and show this on request. All contractors will need to sign in and sign out at the office.

Staff should ensure that windows and external doors are locked when a classroom or office is empty, and at the end of school, and that offices, filing cabinets and cupboards are also kept locked if required.

Any security concerns including break-ins and loss of computer equipment must be reported to the Headteacher and the Police.

**11. Email Security**

Staff must bear in mind that email is a formal record of correspondence and can be subject to request under Data Protection and Freedom of Information legislation – emails are also retained as records on staff, pupil and school files.

Staff must not send anything which would be unlawful or discriminatory, or whose content is defamatory or libellous. Work emails should not be used for forwarding chain letters or similar ‘spam’.The Telecommunications Act 1994 makes it an offence to transmit messages or other matter via a public telecommunications system that is indecent, obscene or menacing. This includes causing annoyance, inconvenience or needless anxiety to another by a message that the sender knows to be false

If members of staff receive an email which breaches the Trust’s policies or breaks the law they are advised to speak to a senior staff member of staff or the IT Director before responding. This includes ‘spam’ emails, particularly those purporting to be from banks, or any email asking the recipient for money.

Staff should re-read any message before sending, checking for clarity and content (including grammar), and ensure that the message is being sent to the appropriate recipient.

Do not use email if the information being sent is personal or confidential, unless you are certain the information will be secure for example through password protection.

Do not use email to anyone who is known not to check emails regularly, or where a phone call or meeting would be a more appropriate way to get the message across.

Do not use email where there may be a contractual or legal need to provide a written and signed document or prove the identity of the sender.

**12. Internet security**

Access to the Internet must be used responsibly and legally. Staff must not take any action which could bring the Trust into disrepute, cause offence, interfere with the organisation's work or jeopardize the security of data, networks, equipment or software.

Under no circumstance should staff make use of the school internet to access chat lines or similar services.

With the advent of e-commerce, staff should beware of committing the school to purchase or acquire goods or services without proper authorisation. Purchase orders must be raised for all goods and services.

A Privacy Impact Assessment must be referred to the DPO / IT Director for all new software systems in advance of their procurement.

Staff must not attempt to download or install unauthorised software from the internet.

Staff should be aware that, as with paper sources, not all information on the internet is accurate, complete or reliable. Users should ensure its validity, as they would printed publications, before using it.

At any time and without prior notice, the Trust reserves the right to examine e-mail, personal file directories, and other information stored on the Trust network and equipment. Permission to examine such information will only be granted by the Chief Executive Officer.

**13. Security of records**

Access to data, and particularly personal data, should be limited to staff who have a genuine ‘need to know’. Staff should be aware that all computer systems permit audit trails to be checked to see who has altered or updated data.

Changes to data, and particularly personal data, should be carried out promptly and recorded appropriately so the reason for the change and its originator is known.

Records should be properly managed to enable staff to find or identify information quickly and accurately. Best practice dictates that student and staff records are kept in one location – multiple locations will lead to duplication or discrepancies between files.

**[New]** **14.** **User training and awareness**

All employees, governors and Directors with access to the Trust’s IT network will be required to undertake NCSC Cyber Security Training upon induction which is refreshed every year.

**[New] 15. Cyber-security incidents**

All cyber-security incidents will be managed in line with the Trust’s Cyber Response Plan.

Any individual that discovers a cyber-security incident will report this immediately to the headteacher and the Chief Executive Officer. The CEO will seek clarification from person notifying incident and convene the Cyber Recovery Team and enact the Cyber Response Plan.

**16. Reporting & responding to security breaches**

In the event of a suspected data breach we will follow the procedures detailed at **Appendix 2.**

A security breach would be caused when [and this not an exhaustive list]:

* A laptop containing personal data is lost or stolen
* A USB [memory stick] containing personal data is lost or stolen
* A vehicle containing a laptop or paper files is stolen
* A laptop or paper files are stolen from a private property
* An email is sent [either internally or externally] with files attached containing personal data and the email is sent to the wrong email address
* An email is sent [either internally or externally] with files attached that contain personal data which is far in excess of that necessary in order for the business function to be carried out
* An email is sent [either internally or externally] which should be sent “bcc” to a large number of people, is instead, sent “to” so the recipient is aware who else has received the email and their personal email address or other personal details
* Personal data is shared outside of the school for a legitimate business reason, but it is lost by the recipient, or it is stolen from the recipient, or it is used by the recipient in a manner for which they have no authority for
* Personal data is transferred electronically outside the school and is not encrypted when it should be
* Paper files of personal data are left unattended and are taken or copied and then used for an unauthorised purpose
* A member of staff uses personal data for a personal rather than a school or Trust business reason

Any theft from the school should be notified to the police.

Any loss of or damage to technical equipment should be notified to the ICT service.

The Data Protection Officer with support from the Trust Business Manager and ICT Manager for cases involving breaches of IT security will investigate the security breach / loss of data through the process detailed at **Appendix 3**. The investigation will determine whether to notify the Information Commissioner. The following guidance will be followed when considering a referral to the Information Commissioner [Notification of data security breaches to the ICO](https://ico.org.uk/for-organisations/report-a-breach/)

**17. Monitoring and review**

This plan will be reviewed by the DPO on a regular basis. The next scheduled review date for this plan is January 2028.

**Appendix 1**

**ORGANISATIONAL & TECHNICAL SECURITY MEASURES**

**Passwords & User Accounts**

* Every user of the system has their own unique username.
* Where possible, we do not use vendor-supplied password defaults for system passwords and other security parameters
* Every user of the system has their own unique password.
* All system passwords are a minimum of 8 characters and must include upper and lowercase letters as well as numbers.
* If several unsuccessful log in attempts are made the account is locked temporarily.
* All unnecessary passwords and user accounts e.g. default logins for computers are disabled or removed.
* Once a user of the system leaves the organisation their account is disabled and removed.
* All staff and system accounts make use of Multi-Factor Authentication.

**Physical Security**

* Where possible, servers are located in a locked server room with restricted access to the key.
* All removable media e.g. USB Memory Sticks, on all computers are restricted from being used.
* Where possible, laptops are encrypted to prevent unauthorised access in the event of a loss / theft.
* We restrict access to data on a business need-to-know basis
* We restrict access to physical records and data ensuring records are locked away with restricted key access
* We operate a records retention schedule to ensure that we do not keep data longer than is necessary

**Network Security**

* We install and maintain a firewall configuration to protect data
* We use and regularly update our antivirus software
* We regularly run scans and ensure that software is kept up to date.
* We remain vigilant against ongoing threats and vulnerabilities through a programme of testing and maintenance.
* We monitor access to network resources
* We regularly test security systems and processes
* We maintain and audit an Information Security Policy that includes a defined process to report and investigate data losses.
* We use spam protection on our email platform to help prevent phishing and email based threats

**Appendix 2**

**Personal Data Breach Procedure**

This procedure is based on [Personal data breaches: a guide | ICO](https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/) produced by the ICO.

* On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify their Headteacher / Principal by completing and submitting the Information Security Incident Report Form (see **Appendix 3**) who will then inform the DPO.
* The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  + Lost
  + Stolen
  + Destroyed
  + Altered
  + Disclosed or made available where it should not have been
  + Made available to unauthorised people
* The DPO will alert the CEO
* The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
* The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
* The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people’s rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  + Loss of control over their data
  + Discrimination
  + Identify theft or fraud
  + Financial loss
  + Unauthorised reversal of pseudonymisation (for example, key-coding)
  + Damage to reputation
  + Loss of confidentiality
  + Any other significant economic or social disadvantage to the individual(s) concerned

If it’s likely that there will be a risk to people’s rights and freedoms, the DPO must notify the ICO.

* The DPO will investigate the incident and document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. The investigation will be recorded using the Investigation Form attached at **Appendix 3**. Documented decisions are retained by the DPO.
* Where the ICO must be notified, the DPO will do this via the [‘report a breach’ page of the ICO website](https://ico.org.uk/for-organisations/report-a-breach/) within 72 hours. As required, the DPO will set out:
  + A description of the nature of the personal data 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 personal data breach
  + A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
* If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
* The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  + The name and contact details of the DPO
  + A description of the likely consequences of the personal data breach
  + A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
* The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
* The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  + Facts and cause
  + Effects
  + Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be retained by the DPO.

The DPO and CEO together with the Headteacher / Principal will review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

**Actions to minimise the impact of data breaches**

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

For data breaches involving disclosure of sensitive information by email we will adopt the following procedure:

**Sensitive information being disclosed via email (including safeguarding records)**

* If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
* Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
* If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
* In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
* The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
* The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

**APPENDIX 3**

**INFORMATION SECURITY INCIDENT REPORT**

To be completed by the person reporting incident.

**Incident report**

Date of incident:

Place of incident:

Name of person reporting incident:

Contact details: email; telephone/address:

Brief description of incident or details of the personal information lost including:

* The categories and approximate number of individuals concerned
* The categories and approximate number of personal data records concerned

Brief description of any action taken at the time of discovery or to be taken including recovery to deal with the breach and to mitigate any possible adverse effects on the individual(s) concerned.

**Appendix 3**

**INVESTIGATION**

**Assessing the risks and actions to be taken**

The Trust Business Manager will liaise with the Governance Manager and where necessary the ICT Manager and Information Asset Owners to consider the following risk factors when assessing, managing and investigating the incident. This list is not intended to be prescriptive and other relevant factors and issues should be recorded as necessary

**Incident summary**

Summary of the actual or suspected security breach

Date of incident:

School(s) / services affected:

People involved in/affected by the incident, (such as staff members, students, contractors, external clients)

Does the incident need to be reported immediately to the police?

YES/NO

**Risk Factor Details and action required**

|  |  |
| --- | --- |
| Which IT systems, equipment or devices  are involved in the security breach?  What information has been lost or  compromised? |  |
| How much information has been lost?  Is the information unique? |  |
| If the incident involves the loss of a laptop  or portable device how recently was the  information it held backed up onto central IT  systems? |  |
| How important is the information or system to the School/Trust? |  |
| Is it business-critical? Do users rely on  access to this particular information asset or can they use reliable electronic copies or alternative manual processes e.g. paper files if the information asset is unavailable? |  |
| How urgently would access need to be  restored to an information asset to resume  business or, if a workaround will keep business moving in the short term, to return to the required standard of service? |  |
| Will the loss or compromise of the information have adverse operational,  research, financial legal, liability or  reputational consequences for the  School/Trust or third parties? |  |
| Is the information bound by any contractual security arrangements? |  |
| Is any of the information confidential?  Please provide details of any types of  information that fall into any of the following  Special Categories of data:   * race * ethnic origin * politics * religion * trade union membership * genetics * biometrics (where used for ID purposes) * health * sex life; or sexual orientation. |  |
| Information that could be used to commit  identity fraud such as personal bank  account and other financial information and national identifiers, such as national insurance numbers and copies of passports and visas. |  |
| Personal information relating to vulnerable adults and children. |  |
| Detailed profiles of individuals; including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed. |  |
| Spread sheets of marks or grades obtained by students, information about individual cases of student discipline. |  |
| Sensitive negotiations which could adversely affect individuals. |  |
| Security information that would compromise the safety of individuals if disclosed. |  |
| Any other personal information that would  cause damage or distress to individuals if  disclosed without their consent  Other categories of “high risk”  Information. |  |
| Information received in confidence e.g.  legal advice from solicitors, trade secrets  and other proprietary information received  from contractors, suppliers and partners  Information that would substantially prejudice the Trust or another party’s intellectual property rights, commercial interests or competitive edge if it were disclosed. |  |
| Information that would compromise the security of buildings, equipment or assets if disclosed. |  |
| **Who else needs to be informed** |  |
| Reported to Police? | YES/NO  If YES notified on  Incident ref: |
| Major risks escalated to the CEO and Audit Committee and Risk Management Register | YES/NO  If YES: Date |
| Notification to Information  Commissioner's Office | YES/NO  If YES notified on [date] |
| Notification to data subjects | YES/NO  If YES notified on [date] |
| Notification to other relevant third parties who can help mitigate the loss to individuals, for example, insurers, banks or credit card companies | YES/NO  If YES notified on |

**Reviewing the incident**

The Responsible Officers should meet to review the incident, ensure that all appropriate actions have been taken to mitigate its impact of the incident and to identify further action needed to reduce the risk of a future breach of this kind

|  |
| --- |
| How and why the incident occurred |
|  |
| Actions taken to resolve the incident and manage its impact |
|  |
| Impact of the incident  (Operational, financial, legal, liability, reputational) |
|  |
| Risks of other adverse consequences of the incident  (Operational, financial, legal, liability, reputational) |
|  |
| Any further remedial actions required to mitigate the impact of the breach |
|  |
| Actions recommended to prevent a repetition of the security breach |
|  |
| Resource implications or adverse impacts, if any, of these actions |
|  |