CARMEL EDUCATION TRUST
INFORMATION SECURITY POLICY

Document Management:	
Date Policy Approved:	29 April 2015
Date Amended:	May 2018
Next Review Date:	May 2021
Version:	2.0
Approving Body:	Resources Committee

Information Security Policy

1. Introduction

1.1 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 Data Protection Policy and the Acceptable Use Policy.

2. Policy Statement

2.1 The Carmel Education Trust is committed to the protection of information and administrative resources, including paper and electronic resources and the media in which they are stored or transmitted.

2.2 The Trust will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.

2.3 The Trust will make every effort to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

2.4 The Trust will ensure all personal data is obtained fairly in accordance with the "Privacy Notice" and lawfully processed – See Data Protection Policy.

2.5 To ensure confidentiality, information will be protected against unauthorised access and only authorised personnel will modify it.

2.6 Security measures such as encryption and password protection for electronic media, and secure storage for hard copy material should be provided to protect against theft or loss.

2.7 Staff will receive training and guidance to enable them to understand, and appropriately apply, security measures for the protection of all information.

2.8 Regulatory and legislative requirements as included within the Data Protection Act 1998 and the Data Protection Act 2018 (once Royal assent is received), the Freedom of Information Act 2000, and the Education (Pupil Information) (England) Regulations 2005 will be met. This may include sharing personal data where it is fair and lawful to do so.

2.9 The Headteacher / Principal of School is the Senior Information Risk Owner for their respective schools and have day to day responsibility for managing information security within their school. The Chief Executive Officer is the overall Information Risk Owner and has responsibility for the implementation of this policy and the management of information security across the Trust. The Data Protection Officer has overall responsibility for monitoring / maintaining this policy and accompanying guidance and providing advice and guidance on implementation.

2.10 Staff are responsible for implementing the policy in their areas of responsibility.

2.11 It is the responsibility of every employee to adhere to this policy.

2.12 This policy and the accompanying guidance will be reviewed, and if necessary updated, every three years.

3 Security and care of equipment

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

3.2 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.

3.4 If the equipment is lost or stolen then the Head of School 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.

3.5 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.

4 Security of data

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

4.2 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.

4.3 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 the school, 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.

4.4 The primary copy of school 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.

4.5 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.

4.6 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.

4.7 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). 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.

4.8 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.

4.9 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.

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

4.11 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.

5. Secure Disposal

5.1 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.

5.2 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 ICT Manager. Discs, memory sticks and other removable devices should be destroyed if they are intended for disposal.

6. Security of buildings

6.1 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.

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

6.3 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.

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

7. Email Security

7.1 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.

7.2 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

7.3 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 ICT Manager before responding. This includes 'spam' emails, particularly those purporting to be from banks, or any email asking the recipient for money.

7.4 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.

7.5 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.

7.6 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.

7.7 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.

8 Internet security

8.1 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.

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

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

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

8.5 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.

8.6 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.

8 Security of records

8.1 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.

8.2 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.

8.3 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.

9 Reporting & responding to security breaches

9.1 In the event of a suspected data breach we will follow the procedures detailed at **Appendix 1.**

9.2 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" and 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

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

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

9.5 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 2**. 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

Appendix 1

Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches 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 2**) 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 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 2

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 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