Information risk management policy

Data hosted by third party service providers

We need to be satisfied that third party, including cloud based services, 'data processors' will treat the information securely as we will be held responsible under the GDPA for what they do with the personal data. We will therefore:
1. Ensure data processors will treat information securely - establish data processing contracts where feasible and ensure they contain necessary data protection related clauses;
2. Establish protocols to allow periodic security reviews of the security arrangements in place to provide assurances of compliance to contract/agreement.

Further information can be found at:
Information security, ICO Guide to data protection
Outsourcing, ICO
Cloud computing, ICO
Model contract clauses: International transfers of personal data, ICO
Model contracts for the transfer of personal data to third countries, European Commission website
Data controllers and data processors: what the difference is and what the governance implications are, ICO

Securely dispose of records and equipment when no longer required.

It is important that we all dispose of paper records and equipment storing personal data securely. We will therefore:
1. Identify and store paper records that contain personal data that require secure disposal in confidential waste bins locked in the offices when not in use.
2. Store equipment or hardware that contained personal data in a locked cupboard whilst awaiting destruction/disposal.
3. Securely dispose of paper records by shredding - ideally a cross cut shredder should be used.
4. Keep a log of all equipment and confidential waste that is sent for disposal or destruction and, where possible, retain certificates of destruction.

Further information can be found at:
IT asset disposal, ICO
Safe computer disposal, Get safe online website

Routinely back-up electronic information to help restore information in the event of disaster.

We need to take regular back-ups to help restore personal data in the event of disaster or hardware failure. We will therefore:
1. Back-up electronic information every ½ term to help restore information in the event of disaster.
2. ensure back-ups are kept in a secure location away from the business premises; and
test the restoration of personal data regularly to check the effectiveness of the back-up process.

Further information can be found at:
Backups, Get safe online website

Log and monitor user and system activity to identify and help prevent data breaches.

Monitoring and logging can help the school to detect and respond to external threats and any inappropriate use of information assets by staff or students. We will therefore:
1. Set up a secure Admin WiFi network that has limited access.
2. Log and monitor user and system activity to identify and help prevent data breaches
3. Monitor inbound and outbound network traffic to identify unusual activity or trends that could indicate an attack.
4. Have a log of user access to systems holding personal data in support of an access control policy, see appendix 1

5. All staff and students using the unsecure WiFi network will be subject to an acceptable usage policy, see appendix 2, and allow their mobile devices to be logged and periodically checked to make sure that their antivirus software and system software is up to date.

Further information can be found at:
Monitoring, 10 steps to cyber security, National Cyber Security Centre
Employment code of practice, ICO

Reporting and recovering from data security breaches.

Purpose

The purpose of an incident response is to ensure that:
1 Data breach events are detected, reported, categorised and monitored consistently.
2 Incidents are assessed and responded to appropriately.
3 Action is taken to reduce the impact of disclosure
4 Mitigation improvements are made is put in place to prevent recurrence
5 Serious breaches can be reported to the Information Commissioner
6 Lessons learnt are communicated as appropriate and can work to prevent future incidents.
This procedure applies to all staff, partners, shared services, suppliers, contractors, representatives and agents of the Council who process personal data for which Good Apple Education is either the data controller or has an interest in the personal data affected. All staff have a role to play to ensure a safe and secure workplace.

Terminology

In line with International Organisation for Standardisation (ISO) directive on the use of terminology in standards and for the avoidance of doubt the following words have the specific meanings ascribed below when used in this document :
'Shall' or 'Must' denote a mandatory requirement. Deviation from these shall constitute non-conformance
'Shall Not' or 'Must Not' denotes something that is prohibited
'Should' denotes a recommendation that is non-mandatory
'Should Not' denotes something that is not recommended
'May' denotes something that is optional.

INCIDENT MANAGEMENT

Definition

A Data Protection breach is the result of an event or series of events where Personally Identifiable Information (PII) is exposed to unauthorised or inappropriate processing that results in it's security being compromised The extent of damage or potential damage caused will be determined by the volume, sensitivity and exposure of the PII. Breach management is concerned with detecting, reporting and containing incidents with the intention of implementing further controls to prevent the recurrence of the event. Examples of common incidents are listed below:
Technical Data Corruption: Malware, Corrupt Code, Hacking
Physical: Unescorted visitors in secure areas, Break-ins to sites, Thefts from secure sites, Theft from unsecured vehicles/premises, Loss in transit/post, Human Resources Data Input errors, Non-secure disposal of hardware or paperwork, Unauthorised disclosures Inappropriate sharing

The proforma in appendix 3 is to be used for the reporting of ALL suspected data protection breaches

A culture in which data protection breaches are reported should be fostered. Although sanctions cannot be totally ruled out, the key objective is develop valuable insight into how such events occur and staff need to be assured that reporting a breach will not in itself result in disciplinary action.

OUTLINE PROCEDURE FOR INCIDENT HANDLING

Investigation

Once a breach has been reported in the form of appendix 3 the following actions must be carried out as soon as possible:
1 Create an entry in the Schools Personal Data Incident Log using the information provided by the reporter
2 Create a folder under Data Breaches using the following format – PB[Breach Reference Number]
3 Start an investigation report and save it in this folder together with any emails/documents relating to the breach.

4 Consideration must be given to notifying the individual(s) affected by the breach. Factors to consider include
a Sensitivity of Information
b Volume of information
c Likelihood of unauthorised use
d Impact on individual(s)
e Feasibility of contacting individuals
Any notification must be agreed by senior managers and the investigation report begun and complete as soon as possible

INCIDENT REVIEW
A key part of data protection breach management is a process of continual review to provide an update on the progress of any investigation, discuss possible recommendations and consider whether specific incidents should be reported to the ICO.

RECOMMENDATIONS
Regardless of the type and severity of incident, there will always be recommendations to be made even if it is only to reinforce existing procedures. All recommendations will be assigned an owner and have a timescale by when they should be implemented which has a dual purpose. The first is to ensure that the school puts in place whatever measures have been identified. The second is that where incidents are reported to the ICO, the Council can demonstrate that the measures have either been put in place or that there is a documented plan to do so. This is a recurrent theme of ICO enforcement and it's important that the organisation's procedures reflect this. Identifying recommendations is more than just damage control – the knowledge of what has happened together with the impact is a fundamental part of learning which can then be disseminated throughout the organisation and beyond.

Further information can be found at:
Notification of data security breaches to the ICO, ICO
Incident management, in 10 steps to cyber security, GOV.UK website

Regular information security awareness training for all staff and are aware of and fulfil their information security responsibilities.

Staff with specific security responsibilities or with privileged access to data systems should be adequately trained and qualified as appropriate. We will therefore:
1 brief all staff on their security responsibilities, including the appropriate use of business systems and ICT equipment.
2 train staff to recognise common threats such as phishing emails and malware infection, and how to recognise and report data security breaches.
3 Ensure staff are trained on or shortly after appointment with updates at regular intervals thereafter or when required.

Further information can be found at:
User education and awareness, in 10 steps to cyber security, National Cyber Security Centre
Training checklist for small to medium sized organisations, ICO

Prevention of unauthorised physical access, damage and interference to personal data.

It is important to implement entry controls to restrict access to the premises and equipment and prevent unauthorised physical access, damage and interference to personal data. We will therefore:
1 Access should be restricted to a 'need-to-know' basis only.
2 Have appropriate entry controls including doors and locks, alarms, security lighting or CCTV.
3 Control access within your premises and have effective visitor procedures, e.g. signing-in protocols, name badges and escorted access.
4 Locate equipment or storage facilities housing more sensitive personal data (including servers) in a separate room, protected by additional controls.

Further information can be found at:
Information security, ICO Guide to data protection

Physical security, Get safe online website
Physical security, CPNI website

Protecting records and equipment.

All staff should lock away paper records and mobile computing devices when not in use ('clear desk and equipment'). The school will ensure that there are adequate secure storage facilities provided to store mobile equipment and hardware, as well as paper records and encourage staff to promptly collect documents from printers, fax machines and photocopiers, and ensure these devices are switched off outside business hours.

Further information can be found at:
Information Security, ICO Guide to data protection

Mobile working policy

Use of personal mobile devices: Employees may have the opportunity to use their personal devices for work purposes when authorized in writing, in advance, by the employee and management. Personal electronic devices include, but are not limited to, personally owned cell phones, tablets, laptops and computers. Employees who have not received authorization in writing from management and who have not provided written consent will not be permitted to use personal devices for work purposes. Failure to follow policies and procedures may result in disciplinary action up to and including termination of employment.
Use of company owned mobile devices: Certain employees may be issued a company owned mobile device. Use of these devices is contingent upon continued employment with Good Apple Education and the device remains the sole property of Good Apple Education. Company provided mobile devices are part of a 'family plan' with shared minutes and include data usage. Excessive use of minutes or bandwidth for non-business activity is discouraged and may result in a Payroll deduction for personal usage.
Security: Employees must put a PIN, password or other security measures in place on every device that is used to access company information.
Employees may not use any cloud-based apps or backup that allows company-related data to be transferred to unsecure parties. Due to security issues, mobile devices may not be synchronized to other devices in the employee's home. Making any modifications to the device hardware or software, or installing additional hardware or software, beyond authorized and routine installation updates is prohibited unless approved by the IT department. Employees may not use unsecure Internet sites. Family and friends should not use personal devices that are used for company purposes. Employees whose personal devices have camera, video, or recording capability are restricted from using those functions anywhere in the building or on company property at any time unless authorized in advance by management. An employee may not store information from or related to former employment on the company's device.
Behaviour: While at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of company devices. Company policies pertaining to harassment, discrimination, retaliation, confidential information and ethics apply to the use of personal devices for work-related activities.
Excessive personal calls, e-mails, or text messaging during the work day, regardless of the device used, can interfere with employee productivity and be distracting to others. Employees must handle personal matters on non-work time and ensure that friends and family members are aware of the policy. Exceptions may be made for emergency situations and as approved in advance by management. Mobile devices shall be turned off or set to silent or vibrate mode during meetings, conferences, and in other locations where incoming calls may disrupt normal workflow.
Work Hours: Non-exempt employees may not use their mobile devices for work purposes outside of their normal work schedule without authorization in advance from management. This includes but is not limited to reviewing, sending, and responding to e-mails or text messages, responding to calls or making calls. Employees may not use their personal devices for work purposes during periods of unpaid leave without authorization from management. [Company Name] reserves the right to deactivate the company's application and access on the employee's personal device during periods of unpaid leave.
Privacy: No employee should expect any privacy except that which is governed by law. Good Apple Education has the right, at any time, to monitor and preserve any communications that utilize Good Apple Education's networks in any way, including data, voicemail, telephone logs, Internet use, network traffic, etc., to determine proper utilization, regardless of the ownership status of the device used to access the company's networks. Management reserves the right to review, retain, or release personal and company-related data on mobile devices to government agencies or third parties during an investigation or litigation. Management may review the activity and analyze usage patterns and may choose to publicize this data to

assure that Good Apple Education's resources in these areas are being utilized according to this policy. Furthermore, no employee shall knowingly disable any network software or system identified as a monitoring tool.
Inspection: At any time, the employee may be asked to produce the mobile device for inspection. The purpose of these inspections is to insure that the employee is following company policy.
Safety: Employees are expected to follow applicable state or federal laws or regulations regarding the use of electronic devices at all times. Employees whose job responsibilities include regular or occasional driving are expected to refrain from using their mobile devices while driving. Regardless of the circumstances, including slow or stopped traffic, employees are required to pull off to the side of the road and safely stop the vehicle before placing or accepting a call or texting. The only exception to this stipulation is if the call can be placed or accepted entirely hands-free. Special care should be taken in situations where there is traffic, inclement weather, or unfamiliar areas. Employees who are charged with traffic violations resulting from the use of mobile devices while driving will be solely responsible for all liabilities that result from such actions.
Lost, Stolen, Hacked, or Damaged Equipment: Employees are expected to protect mobile devices used for work-related purposes from loss, damage, or theft. In an effort to secure sensitive company data, employees are required to have remote wipe software (MDM) installed on their mobile devices by the IT department prior to using the devices for work purposes. This software allows all data to be erased remotely in the event the device is lost or stolen. The remote wipe process will remove all programs and data from the phone and reset it to factory defaults. Good Apple Education will not be responsible for loss or damage of personal applications or data resulting from the use of company applications or remote wiping. Employees must notify management immediately in the event their mobile device is lost or stolen. If the mobile device is damaged, the employee must notify management immediately. The employee will be responsible for the cost of repair or replacement.
Employees may receive disciplinary action up to and including termination for damage to company owned mobile devices caused willfully by the employee.
Termination of Employment: Upon resignation or termination of employment, the mobile device will be reset to factory defaults using the remote wipe software. [Company Name] will not be responsible for loss or damage of personal applications or data resulting from the remote wipe.

Further information can be found at:
Home and mobile working, in 10 steps to cyber security, National Cyber Security Centre
Bring your own device (BYOD), ICO

Configuring new and existing hardware to reduce vulnerabilities and provide only the functionality and services required.

The default installation of ICT equipment can include vulnerabilities such as unnecessary guest or administrative accounts, default passwords that are well known to attackers, and pre-installed but unnecessary software. These vulnerabilities can provide attackers with opportunities to gain unauthorised access to personal data held in business systems. We will therefore:
1 Ensure that are new and existing hardware is configured to reduce vulnerabilities and provide only the functionality and services required.
2 Maintain an up-to-date inventory of ICT equipment.

Further information can be found at:
Secure configuration, in 10 steps to cyber security, National Cyber Security Centre
A practical guide to IT security, ICO
Unnecessary services and default credentials, in Protecting personal data in online services, ICO

The use of removable media.

Removable media (for example, CD/DVDs, USB drives, smartphones) is highly vulnerable to theft or loss, and uncontrolled use can lead to data leakage. We will therefore:
1 Minimise and encrypt personal data stored on mobile devices
2. Ban the use of mobile devices unless authorized by the data protection officer.
3. Log all use of removable media

Further information can be found at:
Removable media controls, in 10 steps to cyber security, National Cyber Security Centre

Assign user accounts to authorised individuals, and to manage user accounts effectively to provide the minimum access to personal data held in information systems.

It is important that we limit access to personal data held in information systems. We will therefore:
1 Restrict user permissions to the absolute minimum.
2 Assign each user with their own username and password to ensure accountability.
3 Have role based user profiles and access levels to ensure that access is only given to those roles that require it in order to complete their work.
4 Review all network and data user access lists at least annually.

Further information can be found at:
User access control, in Cyber essentials scheme, GOV.UK website
Managing user privileges, in 10 steps to cyber security, National Cyber Security Centre
Information access management, Get safe online website
Password storage, in Protecting personal data in online services, ICO

Password security procedures

Areas for focus/suggested actions

Users' access credentials (e.g. a username and password or passphrase) are particularly valuable to attackers. A 'brute force' password attack is a common threat so we will therefore:
1 Enforce regular password changes to all users of both WiFi networks.
2 Enable and actively encourage your users to choose a strong password, at least 8 characters containing both letters and at least 2 numbers.
3 Enforce that passwords are not written down or recorded in accessible locations/systems logs.

Further information can be found at:
Managing user privileges, in 10 steps to cyber security, National Cyber Security Centre
Information access management, Get safe online website
Password storage, in Protecting personal data in online services, ICO

Effective anti-malware defences to protect computers from malware infection

Computers can be infected with malware (for example, viruses, worms, Trojans, spyware) via email attachments, websites and removable media. This can result in the loss or corruption of personal data. We will therefore:
1 Install malware protection software to regularly scan your computer network in order to detect and prevent threats.
2 Make sure the software is kept up-to-date.
3 Educate users about common threats.
4. Have a firewall that is kept up to date.
Further information can be found at:
Malware prevention, in 10 steps to cyber security, National Cyber Security Centre
Viruses and spyware, Get safe online website
Network security, in 10 steps to cyber security, National Cyber Security Centre
Inappropriate locations for processing personal data, in Protecting personal data in online services, ICO

Appendix 2 - Acceptable Usage Policy

This Acceptable Usage Policy covers the security and use of all Good Apple Education's information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all Good Apple Education's employees, contractors and students (hereafter referred to as 'individuals'). This policy applies to all information, in whatever form, relating to Good Apple Education's business activities, and to all information handled by Good Apple Education relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by Good Apple Education or on its behalf.

Computer Access Control – Individual's Responsibility

Access to the Good Apple Education's IT systems is controlled by the use of passwords and are uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Good Apple Education's IT systems.

Individuals must not:

· Allow anyone else to use their user password on any Good Apple Education's IT system.
· Leave their user accounts logged in at an unattended and unlocked computer.
· Use someone else's user ID and password to access Good Apple Education's IT systems.
· Leave their password unprotected (for example writing it down).
· Perform any unauthorised changes to Good Apple Education's IT systems or information.
· Attempt to access data that they are not authorised to use or access.
· Exceed the limits of their authorisation or specific business need to interrogate the system or data.
· Connect any non- Good Apple Education authorised device to the Good Apple Education network or IT systems.
· Store Good Apple Education data on any non-authorised Good Apple Education equipment.
· Give or transfer Good Apple Education data or software to any person or organisation. outside Good Apple Education without the authority of Good Apple Education. Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Internet and email Conditions of Use

Use of Good Apple Education internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Good Apple Education in any way, not in breach of any term and condition of employment and does not place the individual or Good Apple Education in breach of statutory or other legal obligations. All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

· Use the internet or email for the purposes of harassment or abuse.
· Use profanity, obscenities, or derogatory remarks in communications.
· Access, download, send or receive any data (including images), which Good Apple Education considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
· Use the internet or email to make personal gains or conduct a personal business.
· Use the internet or email to gamble.
· Use the email systems in a way that could affect its reliability or effectiveness, e.g. distributing chain letters or spam.
· Place any information on the Internet that relates to Good Apple Education, alter any information about it, or express any opinion about (Acme Corporation), unless they are specifically authorised to do this.
· Send unprotected sensitive or confidential information externally.
· Forward Good Apple Education mail to personal non-Good Apple Education email accounts, e.g. a personal Hotmail account.
· Make official commitments through the internet or email on behalf of Good Apple Education unless authorised to do so.
· Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
· In any way infringe any copyright, database rights, trademarks or other intellectual property.
· Download any software from the internet without prior approval of the IT Department.
· Connect Good Apple Education's devices to the internet using non-standard connections.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, Good Apple Education enforces a clear desk and screen policy as follows:

· Personal or confidential business information must be protected using security features provided for example secure print on printers.
· Computers must be logged off/locked or protected with a screen locking mechanism

controlled by a password when unattended.
· Care must be taken to not leave confidential material on printers or photocopiers.
· All business-related printed matter must be disposed of using confidential waste bins or shredders.

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:
· Working away from the office must be in line with Good Apple Education's) remote working policy.
· Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
· Laptops must be carried as hand luggage when travelling.
· Information should be protected against loss or compromise when working remotely or accept reverse charge calls from domestic or International operators, unless it is for business use.

Actions upon Termination of Contract

All Good Apple Education equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Good Apple Education at termination of contract. All Good Apple Education's data or intellectual property developed or gained during the period of employment remains the property of Good Apple Education and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

All data that is created and stored on Good Apple Education's computers is the property of Good Apple Education and there is no official provision for individual data privacy, however wherever possible Good Apple Education's will avoid opening personal emails.
IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Good Apple Education has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse. Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.
This policy must be read in conjunction with:
· Computer Misuse Act 1990
· Data Protection Act 1998

It is your responsibility to report suspected breaches of security policy without delay to your line management, the IT department, the information security department or the IT helpdesk.
All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Good Apple Education's disciplinary procedures.

Appendix 3 – Data Protection Breach Reporting Form

The aim of this document is to ensure that in the event of a security incident such as data loss, all information can be gathered to understand the impact of the incident and what must be done to reduce any risk to customers and/or CBC data and information and the individuals concerned.

The checklist can be completed by anyone with knowledge of the incident. It will also require review by the FOI & Privacy Specialist who can determine Data Protection Act implications and assess whether changes are required to existing business processes.

1. Summary of Incident	
Date and Time of Incident	
Number of people whose data is affected	
Department	
Nature of breach e.g. theft/disclosed in error/technical problems	
Description of how breach occurred	

2. Reporting	
When was breach reported?	
How you became aware of the breach:	
Has FOI & Privacy Specialist been informed (74968):	

3. Personal Data	
Full description of personal data involved (without identifiers);	
Number of individuals affected:	
Have all affected individuals been informed:	
If not, state why not:	
Is there any evidence to date that the personal data involved in this incident has been inappropriately processed or further disclosed? If so, please provide details:	

4. Data Retrieval	
What immediate remedial action was taken:	
Has the data been retrieved or deleted? If yes - date and time:	

5. Impact	
Describe the risk of harm to the individual as a result of this incident:	
Describe the risk of identity fraud as a result of this incident:	
Have you received a formal complaint from any individual affected by this breach? If so, provide details:	

6. Management	
Do you consider the employee(s) involved has breached information governances policies and procedures:	
Please inform of any disciplinary action taken in relation to the employee(s) involved:	
Had the employee(s) completed data protection training:	
As a result of this incident, do you consider whether any other personal data held may be exposed to similar vulnerabilities? If so, what steps have been	

taken to address this:	
Has there been any media coverage of the incident? If so, please provide details	
What further action has been taken to minimise the possibility of a repeat of such an incident? Please provide copies of any internal correspondence regarding any changes in procedure:	