Policy No:

GIG 04

Policy and Procedure on

Information Security

Policy Author / Reviewer	Paul Follan
Approval Date	Feb 2019
Next Review Date	Feb 2021
Version No	4
Policy Level	Group
Staff Groups Affected	All Staff

Contents

1. Monitoring and Review

1.1 The Proprietor will undertake a formal review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than two years from the date of approval shown above, or earlier, if significant changes to the system and arrangements take place, or if legislation, regulatory requirements or best practise guidelines so require.

Signed

John Ivers

Proprietor

Terminology

2.1. Our aim is to consistently use the following terminology throughout this policy:

'Establishment' or 'Location	this is a generic term which means the Children's Home/school/college
Individual	means any child or young person under the age of 18 or young adult between the ages of 18 and 25
Service Head / Head of Service	This is the senior person with overall responsibility for the Location.
Key Worker	Members of staff that have special responsibility for Individuals residing at or attending the Establishment.
Parent, Carer, Guardian	means parent or person with Parental Responsibility
Regulatory Authority	Regulatory Authority is the generic term used in this policy to describe the independent regulatory body responsible for inspecting and regulating services.
Social Worker	This means the worker allocated to the child/family. If there is no allocated worker, the Duty Social Worker or Team Manager is responsible.
Placing Authority	Placing Authority means the local authority/agency responsible for placing the child or commissioning the service
Staff	Means full or part-time employees of Cambian, agency workers, bank workers, contract workers and volunteers.

3. Purpose

3.1 This policy affects all staff. It policy deals with information security and how it applies to all the appropriate activities throughout the Group and its Locations.

3.2 It is intended to safeguard the interests of Cambian's residents and employees by protecting them from access to unsuitable material access through Cambian's IT systems and to protect Cambian's own interests. It also sets out the steps which must be undertaken in the case that there is any actual, suspected or possible breach of security.

3.3 The aim of the policy is to ensure the security and confidentiality of all information assets, information systems, applications, networks and hardware owned or controlled by Cambian. This will be achieved by:

- Ensuring that all employees are aware of and comply with relevant legislation and principles
- Ensuring that IT Department employees understand the need for security and confidentiality of data and that a culture of security is developed and enhanced.

3.4 Cambian will take seriously any actual, attempted or suspected infringement of the policies in this and other documents, and may take disciplinary action against any employee acting or attempting to act in breach of them. at a culture of security is developed and enhanced.

4. Policy

4.1. This document sets out the Information Security Policy which applies within the IT operational area of Cambian group. It contains the policy and practical information relating to Asset Management, Access Control, Network Security, Mobile Computing and Information Security Event reporting and management.

4.2. This document should also be considered in the context of the overall Information Governance framework of policies.

4.3. Whilst the separate policy document GIG 07 - Information Acceptable Use Policy (AUP) is targeted at all of Cambian's IT users, this document should be seen as complementary to it and provides details of the underlying policy and the environment on which the AUP is based. This document is therefore aimed primarily at the IT Department, who are responsible for providing the necessary tools and controls to enable the requirements of the AUP to be satisfied.

4.4 The IT Department employees are also bound by the separate GIG 7 - Information Systems AUP, and the provisions of this document should be considered supplementary to and not replacing the provisions of that document. This document does not restate the provisions of the AUP except insofar as it describes the manner in which the technical aspects of that policy are brought about. controls to enable the requirements of the AUP to be satisfied.

4.5. These policy and procedures apply to all information, information systems, networks and applications at all Cambian establishments, to all Cambian employees and system users and to any third party Service Providers used by Cambian.

4.6. In this document the term 'employees' should be understood to mean Cambian permanent employees and any contracting or temporary employees or service providers.

4.7. Responsibility for Information Security lies with the Senior Information Risk Officer and the Information Governance Steering Group.

4.8. Responsibility for implementation and maintenance of this policy lies with the Information Security Manager.

4.9. Responsibility for the security of specific IT and Information Assets lies with the designated owner of the asset.

4.10. Responsibility for the practical implementation of the policies in this document lies with individual members of the IT Department charged with carrying out specific tasks. Please note that responsibilities will apply to local ICT Technicians, Central IT Personnel and ITLAB Technical Staff.

4.11. Responsibility for management of Security events varies depending on the nature and severity of the incident. For low-level incidents, such as software malfunctions, these may be managed at the IT Helpdesk level. For more serious events, the Information Security Manager, Data Protection Officer, Caldicott Guardian or SIRO may take responsibility. The procedure for Information Security Event Reporting and Management is below.

5. Procedures

5.1. Cambian's right of access to data and systems: Cambian retains the right to access and monitor any and all data on any of its systems in any and all of the applications on those systems. It furthermore retains the right to make use of monitoring and auditing software to support this right.

Minimise security burden:

5.2. Security measures should be as simple and transparent to users as is possible commensurate with the threat they are intended to combat. For example, the fewer IDs and passwords a user must remember, the less the risk that they will have to write them down.

Maximise use of automated central security controls:

5.3. Cambian uses Microsoft Active Directory which has the capability of providing a high degree of control over access to a variety of assets. Where possible, automated processes should be used to ensure, for example, that user passwords are changed on a periodic, systematic basis, and that passwords conform to the company's standards.

Lowest level of access:

5.4. All system users, especially those in IT, should access systems with the lowest level (i.e. least functionality) of access commensurate with carrying out the specific task. IT system users who require elevated access to systems for specific purposes should use that access only when they are actually carrying out some function which requires this form of access and as soon as the task is finished, should sign off and revert to normal access. In addition, any vendor- provided IDs and default passwords which are set when software is delivered or installed should be removed or disabled before the system commences use.

5.5. Service User access to Cambian Data is to be strictly controlled and monitored. Service users are to be denied access on all Data shares and directory structures where they explicitly do not require access. All Service users are to be granted membership of the AD Group GG CES Service Users Asset ownership:

Asset Ownership

5.6. All information assets have designated owners who are responsible for preserving the integrity and security of those assets for which they are responsible. They form the first line of defence against security compromises and it is usually the case that the faster the reaction to a security issue, the less the effect. (Children Services)

Printing, Handling and Disposal of Confidential and PID Information

5.7. Computer based information which is confidential or contains Personal Identifiable Information (PID) should only be printed when it is essential to do so.

5.8. Information which is printed should not be left unattended at a printer for viewing by other persons.

5.9. Where staff are linked to more than one printer they must check documents are being sent to the correct printer. Where secure print functionality is available this must be used. Never send documents to a printer in a common area open to the public or unauthorised people without using the secure print function.

5.10. Printed information is always to be treated with appropriate levels of security and never left for viewing by unauthorized persons. All desks/offices must be cleared of paper containing PID during extended absences during the day or night and must be locked away securely.

5.11. Unwanted Printed material containing confidential or PID information is to be disposed of securely either by shredding in the provided facilities or placing in the confidential waste paper destruction facilities.

5.12. Confidential or PID data is never to be disposed of in waste paper bins.

5.13. In the event that Confidential or PID information is found disposed of within inappropriate waste disposal facilities – the matter is to be raised with a Senior Member of Staff

Backup and recovery

5.14. All data contained on Cambian's in-house systems will be backed up as often as necessary to ensure that the business of Cambian is not significantly disrupted by failures within a system. Data backups will be carried out to both disk (SAN) and tape as appropriate. Data backup are routines are managed by ITLab

5.15. Data stored on individual File + Print Servers located at schools and hospitals are to be backed up daily (Mon-Thu) to the core data centre. This function is the responsibility of ITLAB, however periodical checks by ICT Technicians/Central IT Staff are to occur to ensure that data backup routines are as expected with no loss of data. ITLAB will maintain electronic records to identify success/fail of core and local server backup routines.

5.16. Daily copies of Backups are held on disk/tape as necessary at the data centre. A weekly tape backup of data is held off site at Iron Mountain secure data facilities.

5.17. A log of backups and recoveries will be maintained and all media will be marked in an unambiguous manner to ensure the correct sequence is followed.

5.18. Backup procedures should be tested periodically on a random basis, but with no longer than 2 months between tests. This will consist of carrying out a restoration of random files to a designated directory. These tests will be carried out by Cambian's nominated IT Services subcontractor (Currently ITLAB) and the results made known during quarterly Service Support Meetings.

5.19. Only IT Department employees or their nominated sub-contractors may undertake restoration of data.

Acceptable Use

5.20. Cambian expects all its employees to use computers reasonably and for the purposes only of Cambian business. All users of Cambian computer systems must note that the Computer Misuse Act 1990 makes it a criminal offence for an unauthorized person to illegally access, attempt such access or misuse a computer.

5.21. Monitoring acceptable use: Cambian will implement and monitor IT systems usage through software which will:

- Monitor internet access made from any of its computers, whether these are used in-house or as part of its mobile inventory.
- Monitor general enduser computer activity as authorised by the CEO in support of internal investigations
- Capture, store, index and retain all email traffic through its servers. Monitoring of ANY Email Account can only be authorised by the CEO or his designated deputy, The Group Company Secretary.
- Ensure that only properly licensed software, acquired by Cambian is deployed on its systems in accordance with the licence conditions.

Monitoring of Email

5.22. The Company reserves the right to monitor employees' e-mails, but will endeavour to inform an affected employee when this is to happen and the reasons for it. The Company considers the following to be valid reasons for checking an employee's e-mail:

- If the employee is absent for any reason and communications must be checked for the smooth running of the business to continue.
- If the Company suspects that the employee has been viewing or sending offensive or illegal material, such as material containing racist terminology or nudity (although the Company understands that it is possible for employees inadvertently to receive such material and they will have the opportunity to explain if this is the case).
- If the Company suspects that an employee has been using the e-mail system to send and receive an excessive number of personal communications.
- If the Company suspects that the employee is sending or receiving e-mails that are detrimental to the Company.

5.23. When monitoring e-mails, the Company will, wherever possible, confine itself to looking at the address and heading of the e-mails. Employees should mark any personal e-mails as such and encourage those who send them to do the same. The Company will avoid, where possible, opening e-mails clearly marked as private or personal.

5.24. The Company reserves the right to retain information that it has gathered on employees' use of e- mail for a period of one year.

5.25. ONLY the CEO can authorise monitoring of an individual's email account. ANY request for an email account to be monitored is to be forwarded in writing or via Email to the Company Secretary at Company Head Office in the first instance.

5.26. Prevention of software installation: Cambian will further restrict end-user modification of systems by using security settings which:

- Prevent installation of any software other than by authorised, qualified IT employees acting with proper authority.
- Prevent user access to computer settings and hardware configurations and these shall only be modified by authorised, qualified IT employees acting with proper authority.
- Where possible, Cambian will prevent access to unsuitable web sites. Cambian will do this through a mix of Internet and Firewall Filtering solutions

Anti-Virus:

5.27. Cambian will maintain Kaspersky Endpoint (antivirus software) on all systems which are potentially subject to attack. IT will ensure that regular updates are being received.

5.28. For all in-house systems connected to the network, this will be kept up to date and refreshed as often as new data is received from the anti-virus software provider.

5.29. For mobile systems, connecting to the Cambian network or direct to the internet will automatically trigger an update to the latest version.

5.30. Anti-Virus – Treatment of e-Mails: Since end users are not permitted under Cambian policy to install software on their systems, any emails containing executable files should be isolated and quarantined automatically. This provision should include files with the extensions .exe, .bat, .scr, .vbs, .eml. Receipt of such files should be treated as a security event and reported accordingly. As this is not a normal method of distributing software upgrades and fixes, even if the file appears to come from a safe source it should be treated with suspicion.

5.31. Anti-Virus Alert: From time to time, warnings are issued of potential internet exploits which may require special attention (e.g. major denial of service or bot attacks). In this case, Cambian will obtain advice from Kaspersky or ITLAB as to the best methods of avoiding adverse effects and put these into action.

Anti-Virus Action

5.32. When a virus alert occurs on a computer the computer will be turned off and isolated from the network.

5.33. IT's responsibilities in this case are to:

- Verify the existence of the virus
- Identify the source of the virus
- Determine the spread of the virus internally and externally
- Obtain the risk assessment of the virus from Kaspersky
- If necessary, disable the WAN until the virus has been eliminated
- Cleanse all infected computers
- Warn any external parties who may have been affected
- appropriate, inform Kaspersky of a new virus.

5.34. A Security Incident report should also be completed.

5.35. If it is suspected that the virus was introduced maliciously then a report is to be submitted to the Information Security Manager detailing the circumstances and effects upon Cambian business practice.

Data Encryption

5.36. Cambian will provide a facility to encrypt files sent by e-mail or transportable media, which are of sufficient strength to resist attacks by non-specialised agencies. This is currently considered to be 128-bit encryption for built-in data security and 256-bit encryption for forwarding data via email or media such as CD and DVD.

5.37. At present, given Cambian's network security controls there is no general requirement for any in-house data to be encrypted.

5.38. Any confidential information sent by email should be sent only once it has been encrypted.

5.39. Company Data is only to be stored on business issued storage devices. These storage devices are limited to Company Servers, desktops, laptops and encrypted USB Devices.

5.40. The storage of data on unencrypted devices is strictly forbidden.

5.41. USB Media Devices will only be issued by the IT Department on an as needed basis. Requests for issue of Encrypted USB Devices are to be processed by the Unit or Individuals Line Manager to the Head of IT.

5.42. USB devices will only be issued to named individuals for use by that individual. Use of USB Departments for generic departmental use is not allowed.

5.43. USB devices are to be encrypted to 256 AES/FIPS 197.

5.44. Use of Personnel USB, CD/DVD, or any portable device for holding or transporting company information whether encrypted or otherwise is strictly forbidden.

Business Continuity/Disaster Recovery

5.45. IT will, in conjunction with other departments, develop, maintain and periodically test a Business Continuity/Disaster Recovery plan. This will identify, assess and evaluate possible incidents and their effect on Cambian and its operations.

5.46. The plan will be developed by the Information Security Manager and will be updated whenever there is a material change in the circumstances of the business (e.g. new premises).

Access Control

5.47. Access to any of Cambian's IT facilities or data is restricted to authorised users only. All access to systems and data will be controlled by means of password-controlled accounts which will be issued to authorised users only.

5.48. Maintenance of software and hardware related to access control will be carried out by members of the IT Department or authorised vendor employees under the supervision of members of the IT Department. All changes and updates will be risk assessed in advance and a record of changes will be maintained which will include the names of those responsible and dates undertaken.

5.49. These accounts will be maintained in a security environment based on Microsoft's Active Directory (AD). This will be maintained in a manner which is sufficiently granular as to allow users to be allocated just such access rights as they need to carry out their responsibilities. Access to the AD change facilities should be tightly restricted and limited to named individuals with security responsibility.

5.50. This approach should allow the minimisation of the number of IDs and passwords required. In general, a non-IT user should have a single ID and password which is used for access to all systems and data to which they have legitimate access.

5.51. New accounts: If a new ID is required for a new or temporary employee, this should be processed as part of the induction process and the request will come from local or central HR. A new user should be allocated appropriate access through AD (Active Directory) and be provided with an ID and a temporary password which can be used once only. The new user will be instructed that they must devise and record a new password as part of their initial sign on to the system.

5.52. Authorisation to use an application or access specific data is controlled and users will be granted access only to such applications and data as they require to carry out their duties.. When applications offer the facility to create different levels of user (e.g. 'Administrator', 'User') this should be used and system users should be granted the lowest level of access commensurate with being able to carry out their duties.

5.53. Account modification: Requests for changes if a system user (including IT employees) requires changes to their access (for example, access to a new application), then a request, agreed by the local Head of Establishment or function manager will be received. If this is in order the change will be made to the AD and logged.

5.54. Retirement and Deletion of accounts: As soon as an employee leaves Cambian's service, or in case of severe disciplinary matters as soon as IT is notified of the requirement, access to the account associated with the person will become restricted such that only IT Department employees can have access. The account will not normally be deleted until three calendar months after the departure of the employee to allow any transfer of data (To include email) or similar activities have been completed. In extenuating circumstances the account may be retained indefinitely if an appropriate business case is raised.

5.55. IT users may need to have more than one form of access in that they may require a normal security level ID for day to day tasks, but an elevated access for systems maintenance purposes. It is mandatory that such elevated access is used ONLY when such tasks are actually being carried out. In all other respects, the elevated account maintenance should be subject to the same restrictions as a normal account.

5.56. Passwords will be maintained according to the rules set out in the Acceptable Use Policy. Passwords must:

- Not be names or have other obvious connection to the user.
- Be changed regularly and not be repeated.
- Be a mixture of letter, numbers and symbols
- Be kept secret.
- Not be shared or disclosed to ANY party, even if they claim to be from IT, management or an external party such as the police.

5.57. Passwords should normally be changed on a regular basis under software control currently by default this is every 42 days.

5.58. Forgotten passwords: If a password is forgotten, a new temporary password may be requested from IT. This will be issued only once IT has determined that the requestor is the correct person associated with the ID for which the password is to be issued. The password issued will be capable of allowing a single access to the system for the purposes of setting up a new password.

5.59. A log of forgotten password requests will be maintained.

5.60. Compromised password: If a user has reason to believe that their access has become compromised by exposure of a password, a new password is to be issued, and the incident recorded as a Security Event.

Network Security

5.61. Access to all of Cambian's networks is restricted to authorised users who are identified in the Active Directory (AD). Any changes to the AD apart from those relating to the maintenance of user accounts will only be carried out after a risk assessment and approval from the Information Security Manager.

5.62. In general, no third party equipment should be attached to Cambian's network. If, for maintenance or upgrade reasons, it becomes necessary to connect non-Cambian owned hardware to Cambian's network, a risk assessment should be carried out. The following courses of action should be considered:

- Can the task be undertaken by disconnecting any Cambian hardware affected from the network?
- Can the task be undertaken on a sub network isolated by firewalls and other security from the rest of the network?
- Can the work be carried out at times when adverse outcomes (i.e. system or network failure) will have least effect?
- Can all Cambian data (or at least confidential data) be isolated from the non-Cambian device?

5.63. Before any connection is permitted, it is essential that:

- The third party company has formally agreed in writing to accept Cambian's terms of security and confidentiality
- The Information Security Manager has given explicit agreement and permission to the connection.

Physical Security

5.64. Access to any IT assets which do not require physical access by end-users will be restricted to just those employees (normally IT Department employees only) who need such access. All assets, such as servers, routers and similar items will be kept in secure facilities.

5.65. Computer users are to ensure that all display screens are placed such so as not to allow for oversight by unauthorised persons.

5.66. Access to such facilities must be strictly controlled and only named individuals will be permitted access. The types of location which require access restrictions of this nature include:

- Server rooms
- Communications rooms
- Communication Cabinets
- Rooms containing patch panels
- Rooms containing switches, routers, firewall hardware machines
- Any other rooms containing IT hardware which does not require end-user access.

5.67. The Information Security Manager is responsible for ensuring that there are suitable environmental controls in place for server and network equipment assets (UPS, air conditioning, fire suppression etc.).

5.68. Where possible, hardware assets will be physically secured in their environment. For example, servers and communications device may be physically placed in a rack and secured with locking devices.

Firewalls

5.69. All Cambian networks will have firewall protection separating them from other networks of differing levels of trust. Firewalls will be used at all interfaces between networks.

5.70. Cambian will monitor internet activity with the use of firewall software/hardware and internet web monitoring software, which provides reports of Internet usage. This will operate in a bi-directional manner, thus protecting data held on Cambian servers from unauthorised remote access (hackers).

5.71. A copy of all firewall rule-sets will be maintained by the IT Department or their nominated subcontractors (Currently ITLAB).

5.72. All firewall rule changes will be subject to a risk assessment (where appropriate) and change-control procedures.

5.73. Access to firewalls is restricted to a limited number of individuals. Any request to gain access to a firewall must be approved by the IT Security Manager.

5.74. Internet access is provided only for business related and educational purposes. Internet access is not provided for private use. Internet access is monitored.

Remote Access

5.75. Remote access is limited to authorised individuals via either SSL VPN or VPN Client and is controlled by access to the necessary Active Directory Group Account which authenticates such remote connections.

5.76. All individuals provided with remote access capability are authorised by the Technical Operations Manager via documented and authorised change control process.

Wireless Networks

5.77. Wireless networks are intrinsically less secure than hard-wired networks and have the potential for being attacked either for illegitimate use or for accessing information assets.

5.78. All wireless networks that allow access to Cambian's corporate network will use WPA authentication and TKIP encryption.

Mobile Computing

5.79. Mobile computing whether from laptop computers, smart phones or other devices capable of storing and / or processing information presents risks and areas of concern in addition to those which apply to in-house systems. All provisions which apply to in-house systems apply equally to laptops and other mobile devices. For example, accounts set up on laptop systems should not give access to system settings, such as BIOS settings, or allow installation of software by non-IT employees.

5.80. Access methods other than secured wireless (including 3G/4G) shall be disabled on all devices capable of using them. This includes Bluetooth, IRDA (infra-red), GPS and any others which may apply.

5.81. Random periodic audits of software and data on laptops should be undertaken and recorded in an audit log. Cambian should supply users with security devices such as Kensington locks, which assist users with the physical security of devices.

5.82. The IT Department should supply users with a suitable protective case for laptop and other mobile device.

5.83. It is understood that mobile users may need to access the Internet and email for personal reasons while travelling. Any Infringement of existing corporate IT policies to include non-appropriate Internet and email usage may be subject to disciplinary procedure.

5.84. When a mobile user connects to Cambian's network, this should enable an update to any anti-virus or other maintenance or security update which is outstanding for that machine.

5.85. Mobile devices (i.e. Laptops, Tablets and Smart Phones) are not to hold original versions of data and as a result there are no facilities provided to back up these devices. Any data is to be stored on the appropriate company servers with only off-line copies held locally only on a mobile device, synchronised whenever possible with a parent server.

Asset Management

New assets

5.86. Requests for new assets will initially be passed to ITLAB and then the Internal Cambian IT Helpdesk for evaluation and approval.

5.87. All IT assets purchased will be recorded. On receipt, the individuating details (e.g. Item number / Licence number) will be recorded in an asset register.

5.88. A register of each hardware asset will be maintained. NOTE: Normally, a PC, or router or similar device will count as 'a hardware asset' rather than, for example a keyboard or a graphics card unless there is something special or unusual about it.

5.89. A new Laptop or Desktop, prior to deployment is to is to be loaded with the relevant corporate system image to ensure baseline standard of IT systems across the Group

5.90. Details of software loaded beyond the baseline image onto each computer will be maintained.

5.91. Each asset, whether hardware or software will be allocated an 'owner', who will be personally identified and who will be responsible for the day-to-day security and maintenance of the asset.

Information Systems Assets

5.92. The nominated owner of each Information System Asset is responsible for:

- Documenting the access control processes and the associated access approval process for the asset
- Conducting a periodic risk assessment on the asset to a programme dictated by the Information Security Manager or Data Protection Officer in accordance with GIG 6: Risk Management Policy and Procedures.

Audit of assets

5.93. A regular (twice yearly) audit of information assets will be conducted. Maintenance of assets

5.94. Only the IT Department or their nominated subcontractors are permitted to carry out maintenance of information assets.

5.95. Faults will be reported by users to the ITLAB Helpdesk via Email or by Telephone. The Helpdesk will record the details of the fault electronically and issue a 'ticket' with a unique reference number. These may consist of (but not be limited to) network access faults, internet access problems, hardware failure, operating system failure.

5.96. No action will be taken on faults until officially reported to the ITLAB Helpdesk and a reference number has been issued, unless the fault is of a severe nature (e.g. server failure). In the case of such failure, the electronic record will be recorded later.

5.97. IT will endeavour to clear major problems with 24 hours. For lesser reported faults, IT will endeavour to repair problems within 5 working days. If the delay to resumption of service is likely to be longer, IT will inform the department involved.

Disposal of assets

5.98. When IT hardware has reached the end of its useful life or is beyond economical repair then arrangements are to be made, by the IT Department, with a reputable source for collection and disposal of such equipment. The authority of the Technical Operations Manager is to be obtained before disposal.

5.99. A certificate of destruction is to be obtained from the disposal company. This certificate is to be retained on file by the IT Department.

5.100. The Asset Register is to be amended to identify the disposal of the equipment.

5.101. In the event of a computer being disposed of all software is to be removed. Where the licence permits the software may be re-used or stored for future use. OEM software will be disposed of with the computer as these licences are non-transferable.

5.102. Prior to disposal all data is to be removed and the hard disk low level formatted. New Information Systems

5.103. The Information Security Manager will ensure that all new information systems, applications and networks will be subjected to a risk assessment to determine the security controls required.

5.104. This evaluation will include, but not be limited to the requirements for:

- Physical security
- Modes of access and network security
- User access permissions and the associated approval processes
- Disaster recovery
- Administration responsibility

5.105. No new system can be put into operation until the plan produced as a result of the risk assessment has been approved by the Information Security Manager.

5.106. In addition and where appropriate, the Information Security Manager will ensure that the impact of any new system on GIG 3: Confidentiality and Data Protection Policy is assessed and has developed guidelines for Privacy Impact Assessments to support this requirement.

5.107. All information security events must be reported in line with the Data Breach Incident handling process (GIG 04.02) and recorded using GIG 4.01 - Incident Report. This sets out the details of an incident. The following table sets out who should be informed depending on the type of incident:

Event description	Initial Notifications				
	IT Helpdesk	Information Security Officer	Caldicott Guardian	Data Protection Officer	SIRO
Damage to information due to flood, fire or other environmental reason	✓	✓	✓	✓	
Loss or theft of computer or mobile computing device (including laptop, tablet or mobile phone)	✓	✓	✓	✓	
Loss or theft of portable media (CD, DVD, USB memory stick)	✓	✓	✓	✓	
Disclosure of business confidential or personal information to wrong person(s) (via Email, Post, Courier,Fax, Verbal)	✓	✓	✓	✓	
Unauthorised disclosure of business confidential or personal information	✓	✓	✓	✓	
Computer Virus Outbreak	✓	✓	✓	✓	
Corruption of electronic information	✓	✓			
Unauthorised changes to personal, clinical or business confidential information	✓	✓	✓	✓	✓

5.108. When an incident is reported, IT should carry out an immediate risk assessment to determine:

- Is there a continuing risk?
- How severe is the risk? (it is better to overestimate severity rather than the reverse)
- Are there any health and safety issues raised by this incident?
- What kind of breach of security (confidentiality/integrity/availability) has occurred?

5.109. The result of this analysis will be recorded.

5.110. Where appropriate, the Information Security Manager, Data Protection Officer and Caldicott Guardian will undertake prompt investigation and risk assessment for each reported event and implement appropriate controls to address the risk.

5.111. The Information Security Manager will report to the Information Governance Lead who, together with the Data Protection Officer, will decide whether the breach should be reported to the Information Commissioner.

6. Standard Forms, Letters and Relevant Documents

6.1. GIG 4.01 – Appendix 1 – Incident Report

6.2 GIG 4.02 – Appendix 2 – Data Breach Incident Handling Process