Information Security Policy

Director Responsible:	**Robert Krawczyk**
Author:	**Bryan Inglis**
Issue Date:	**January 2019**
Version Number:	**2**
Approved by:	**SMT January 2019**
Review Date:	**January 2020**

DOCUMENT HISTORY

Date	Author/ Editor	Summary of Changes	Version No.
28.01.2019	B Inglis	New Policy	1
31.01.2019	R Krawczyk	Adjustment to cross references	2

CONSULTATION AND RATIFICATION SCHEDULE

Name of Consultative Body	Date of Approval
Senior Management Team	
HR and Learning and Development	
Care Coordination Department	

CROSS REFERENCE TO OTHER POLICIES / STRATEGIES

This policy should be read in conjunction with:	Detail
Policy 6	Risk Assessment Policy
Policy 18	Disciplinary Policy
Policy 32	Mobile Phone Policy
Policy 33	Computer Policy

KEYWORDS: information security, asset register, IT systems, security, breach, password, email, confidentiality, data protection

CONTENTS

1. PRINCIPLES

Primecare Health LTD recognises the importance of managing our information in line with its legal and regulatory responsibilities. Primecare Health LTD takes a risk-based approach to ensuring information security and upholding the principles of transparency and accountability, whilst ensuring confidentiality is a primary focus.

Information risk is inherent in most business and administrative activities and all staff will continually manage this as part of their day to day roles. This policy underpins the overall SA (System Administration) Risk Strategy and Policy. The intent is to embed management of information risk into business and operational processes in a practical way, not impose additional requirements to roles and functions.

2. OBJECTIVES

Primecare Health is, as part of an overall Information Governance Programme, focusing on improving the way we manage our organisational information. This will be achieved through improved electronic systems, review of current processes, and supported by robust policy and procedure as well as training/ support for staff.

The objectives related to Information Security are as follows:

- Information will be protected in line with relevant policies, procedures and legislation
- Staff will be aware of and receive training in information security matters
- Ensuring the appropriate availability, confidentiality and integrity of all SA information, regardless of format
- Ensuring that staff have the right level of access to information required to do their jobs
- To protect SA information from unauthorised access
- Ensuring that we understand what information we hold, where it is held and assign ownership for the information by means of an Information Asset register that is regularly reviewed and updated.
- Ensuring that our IT systems support business needs and that we can assure digital continuity

3. FRAMEWORK FOR INFORMATION SECURITY

This policy considers the following areas of Information Risk Management:

- Management framework (to support implementation and monitoring of this policy)
- Asset Management
    - Security relating to IT equipment (e.g. servers, laptops, other devices)
    - Security relating to paper records (e.g. support plan documents, personnel files)
    - Establishing and maintaining an Information Asset register
- Physical security (e.g. access to premises, staff safety, safe use of IT equipment when remote working or travelling)

- Human resource security (linking to good practice in recruitment through to ensuring return of all SA assets at termination of employment)
- Identity and access management – to SA systems (e.g. passwords, appropriate access to information based on business need and role)
- IT Operational security (e.g. ensuring systems and applications support business need and maintain integrity and availability)
- Information Security Incident management (e.g. data breaches, loss of equipment)
- Regulatory Compliance

Specific procedures and guidelines will be compiled to support the management of these aspects of information security. Management of information security must be driven by business need and carried out within relevant legal and regulatory requirements.

4. MANAGEMENT FRAMEWORK

An Information Security Group will be convened. The members of this group will be the same as that of the Policy Sub Group as well as the IT Manager. The Senior Management Team sponsor of this group will be the Director.

The group will:

- Oversee policy and procedure developments
- Oversee the Information Asset Register, appointing relevant Information Asset Owners (IAO) and may be IAOs themselves
- Ensure communication of revised or new procedures and information about training to managers for cascade to staff
- Raise awareness of information security within their areas
- Ensure that breach management procedures are followed and assist with incident investigation as required
- Developing and reporting relevant KPIs

5. ASSET MANAGEMENT

An Information Asset Register (IAR) should document links between information assets and business requirements. The IAR will include details about physical, electronic and paper based records and will support improved Records Management. The Information Security Group will establish an IAR including information about:

IT infrastructure
Hardware, Software/ licences
Support
Format
Owner
Users
Classification of data (e.g. sensitive personal/ personal/ other)
Retention/ disposal
Risks to asset/ risks to business from the asset

Benefits of an IAR include:

- Track and monitor lifecycle and maintenance of equipment
- Will help SA to understand what information is held, where it is held and in what format
- Will help us to identify opportunities for efficiencies, e.g. identify duplication, standardise formats
- Enable selection and deployment of appropriate security controls and access levels
- Will support better information sharing and support requirements related to Subject Access Requests/ Freedom of Information requests
- Bring clarity and enable better adherence to Retention Schedules
- Reduce risk of non-compliance particularly related to DP Principles, e.g. identify IAs that are no longer required
- Enable file structure on networks to be standardised and better managed.
- Reduce risk of loss of data as info is held in right place
- Enable most effective use of network storage capacity

The Information Governance Manager will oversee the IAR and will be responsible for ensuring that regular review takes place, in conjunction with the Information Security Group. It is envisaged that once established the IAR will be reviewed annually.

Standards and procedures for creating, classifying, recording, using and disposing of Information Assets will be established and link to the Records Management Policy and IT Systems Usage Policy.

6. PHYSICAL SECURITY

All Primecare Health sites, equipment and information will be protected using proportionate security controls based on the level of risk. Physical security measures may include:

- CCTV
- Door Entry systems
- Digital or physical locks/ keys
- Lockable secure storage (e.g. filing cabinets, safes)

Access to operational areas and Primecare Health information will be determined by operational need. Access rights should be established and managed locally by managers, for example, staff may be issued with identity cards which should be worn as directed.

Sites shall maintain visitor records and ensure that all visitors are verified at point of entry. Compliance with relevant Health and Safety regulations should be ensured at all sites.

Issue of keys and other assets must be logged and updated as required. Local administrators are responsible for ensuring the upkeep of these registers. Staff who are issued with keys are responsible for their safety. Local managers are responsible for ensuring that staff return keys and all other Primecare Health assets at the end of their employment or change roles or teams.

IT equipment will be issued based on operational need. Please refer to the IT Systems Usage policy regarding security of IT equipment such as phones, laptops and encrypted USB sticks. Particular care of Primecare Health assets must be taken when staff are travelling or working remotely. Damaged IT equipment should be reported to line

management and the IT department. The IAR must be updated when any equipment is disposed of or replaced, or where staff move teams.

Loss of ANY Primecare Health assets or the breach of any Primecare Health premises should be reported under the Security Incident Management procedure.

7. HUMAN RESOURCES SECURITY

Primecare Health wishes to demonstrate its commitment to quality, and an appropriately skilled and vetted workforce forms part of that commitment. Prior to employment, Primecare Health will carry out appropriate identity, reference and other required checks based on regulatory compliance needs. Please refer to the Recruitment Policy. Staff will receive appropriate training on security as required for their role. This will include specific training on Information Security (e.g. Data Protection training) and general risk management.

8. SECURITY OF ACCESS TO PRIMECARE HEALTH IT SYSTEMS

HR will notify IT of new employees to enable the IT Department to create network and e-mail accounts and system permissions. Users will be granted access to the appropriate network areas and systems required to undertake their role. HR will notify IT when an employee leaves the organisation and they will disable network and email accounts immediately to protect Primecare Health's information and systems. Email inboxes will be maintained on the email server until the last day of the month following the date of leaving, whereupon they will be removed.

Data security is also ensured through use of encrypted devices and encrypted emails where required and these are managed, logged and tracked by IT and local administrators.

Staff should not divulge or share passwords with anyone else. Service Users should not be enabled access to Primecare Health records or email accounts, and staff equipment should be kept securely so that unauthorised access does not occur.

When staff change roles within the organisation, access to their previous information may be removed as appropriate, and new access rights established. This would be undertaken by IT on instruction from HR and the staff member's new manager.

Access rights to some systems and applications are managed by department heads, who allocate access via usernames and passwords. These systems include (among others) the Finance, HR and Fundraising systems as well as databases used by the school.

Staff are responsible for maintaining confidentiality of records/ information they access and should be guided by this policy, local management and relevant procedures when working with Primecare Health information.

9. IT OPERATIONAL SECURITY

The IT department will ensure the network infrastructure is robust enough to support business need. They are responsible for purchase and maintenance of all new systems,

equipment, programmes where identified as a business need and will be involved with any tendering process as required.

Business requirements for new or significant changes to IT systems should be managed under Primecare Health's project management processes. Impact assessments, process mapping, user requirements and a full cost/ benefit analysis will inform decision making. Security and privacy elements must be considered as part of the purchasing of any new systems/ equipment.

The IT department also manage security processes and procedures e.g. those relating to backups, firewalls/ virus protection and upgrades to systems. Robust contingency plans are in place to minimise potential disruption and ensure digital continuity.

The IT department is supported by various helpdesks which staff should contact in the event of any issues. The IT department has limited resource and Primecare Health has established helpdesk procedures to allow routine issues to be resolved and maximise efficiency within the IT department.

To ensure systems integrity, legal compliance and reduce the risks of viruses and data loss, staff must not download unlicensed software, including apps, onto any Primecare Health device without permission. Breach of the IT Systems Usage Policy is taken extremely seriously, and staff are likely to be subject to disciplinary procedures where any breach of policy and procedure are recorded.

Some suppliers (e.g. helpdesk, software support specialists) are granted remote access to fix specific programme issues. Staff are advised to close down all other programmes before engaging in a remote session to limit potential access to other Primecare Health information. Staff should not leave their work station but observe the remote session and ensure that the session is properly terminated once the issues are resolved.

10. INFORMATION SECURITY INCIDENT MANAGEMENT

All security incidents or breaches should be reported using the Security Incident Report form – this can be found as part of the Security Incident Management procedure published on Source.

11. REGULATORY COMPLIANCE

Primecare Health complies with various legislation relating to security and confidentiality, for example the Data Protection Act (1998), and the General Data Protection Regulation which will came into effect on May 2018. Primecare Health is also compliant with the Privacy and Electronic Communication Regulations (last revised in 2016).

Primecare Health will report incidents as required to the Information Commissioner's Office. We will also report any security incidents in line with requirements from other regulators such as the Scottish Social Services Council, Care Inspectorate and Education Scotland.

12. OTHER PRIMECARE HEALTH STAKEHOLDERS

Primecare Health aims to be as transparent as possible with supporters regarding the processing of their data. The website displays a privacy notice and information about the use of cookies. All supporters are provided with information about their rights as data subjects, as well as options to unsubscribe from communications. Records are securely stored and managed in line with the Records Management Policy/ Retention Schedule.

Information about service users may be shared with relevant agencies to fulfil regulatory requirements, for example, with relevant Social Workers during reviews. Rights of access to a service user's personal or service-related information will be detailed within their support plan and staff should ensure that they are familiar with the arrangements for the service users they support.

Suppliers to Primecare Health are expected to respect our information and manage it in line with our high standards, and we will adhere to privacy legislative requirements during tender, purchasing and contracting activity. Written data processing agreements will be put in place where necessary and will be monitored by the Commercial Manager.

13. MONITORING AND REVIEW

This Policy will be reviewed every year in line with the organisation's policy review cycle, or earlier if required due to legislative update. This policy may also be updated within the yearly timeframe to reflect progress against objectives related to Information Security management.