Brigstock Skin and Laser Centre

18. Information Management

Document Classification: Policy		**Document No:** 18
Issue No: 01		**Date Issued** 09.07.09
	Author C. Lyons	**Review Date:** 25/06/2020
Revisions:		**[Enter details of revisions below]**
19.10.2010	S. Akram	**Reason for Changes:-** Add in "Requests for urgent paper medical records"
13.8.10	CL	Reviewed document
1.7.11	CL	Reviewed document
27.8.12	CL	Reviewed document

28.8.13	CL	Reviewed document
13.10.14	CL	Reviewed document
24.10.15	CL	Reviewed document
16.12.16	KH	Reviewed document
19/02/2018	CL	**Review**
28/02/2019	CL	**Reviewed and updated**
25/06/2019	NM	**Reviewed**

Table of Contents

18.I NFORMATION GOVERNANCE POLICY 7
18.1.1 Summary 7
18.1.2 Principles 7
18.1.3 Responsibilities 9
18.2 Information Security 10
18.2.1 Introduction 10
18.2.2 Objectives, Aim and Scope 10
18.2.3 Responsibilities for Security 11
18.2.4 Legislation 12
18.2.5 Policy Framework 12
18.2.6 Access Controls 13
18.2.7 User Access Controls 13
18.2.8 Computer Access Control 13
18.2.9 Application Access Control 13
18.2.10 Equipment Security 13
18.2.11 Computer and Network Procedures 13
18.2.12 Security Incidents and weaknesses 13
18.2.13 Protection from Malicious Software 13
18.2.14 User Disks 13
18.2.15 Monitoring System Access and Use 14
18.2.16 Accreditation of Information Systems 14
18.2.17 System Change Control 14
18.2.18 Intellectual Property Rights 14
18.2.19 Business Continuity and Disaster Recovery Plans 14
18.2.20 Reporting 14
18.2.21 Policy Audit 14
18.2.22 Further Information 14
18.2.23 Do's and Don'ts for Users" 14
18.3 Network Security 16
18.3.1 Introduction 16
18.3.2 Aim 16
18.3.3 Network definition 16
18.3.4 Scope of this Policy 16
18.3.5 The Policy 16
18.3.6 Risk Assessment 17

18.3.7 Physical & Environmental Security 17
18.3.8 Access Control to Secure Network Areas 18
18.3.9 Access Control to the Network 18
18.3.10 Third Party Access Control to the Network 19
18.3.11 External Network Connections 19
18.3.12 Maintenance Contracts 19
18.3.13 Data and Software Exchange 19
18.3.14 Fault Logging 19
18.3.15 Security Operating Procedures (SyOps) 19
18.3.16 Network Operating Procedures 19
18.3.17 Data Backup and Restoration 20
18.3.18 User Responsibilities, Awareness & Training 20
18.3.19 Accreditation of Network Systems 20
18.3.20 Security Audits 20
18.3.21 Malicious Software 20
18.3.22 Secure Disposal or Re-use of Equipment 20
18.3.23 System Change Control 21
18.3.24 Security Monitoring 21
18.3.25 Reporting Security Incidents & Weaknesses 21
18.3.26 System Configuration Management 21
18.3.27 Business Continuity & Disaster Recovery Plans 21
18.3.28 Unattended Equipment and Clear Screen 21
18.3.29 Security Responsibilities 22
18.3.30 Registered Manager's Responsibilities 22
18.3.31 Registered Manager's Responsibilities 23
18.3.32 Line Manager's Responsibilities 23
18.3.33 General Responsibilities 24
18.4 User Access Management 25
18.4.1 Introduction 25
18.4.2 User registration 25
18.4.3 Change of user requirements 26
18.4.4 Change of password 26
18.4.5 Removal of users 26
18.4.6 Privilege management 27
18.4.7 User password management 27
18.4.8 Review of user access rights 28
18.5 Computer Internet and Email Usage 29
Introduction 29
18.5.2 APPLICABILITY 29
18.5.3 THE POLICY 29
18.5.5 Email disclaimer 31
18.5.6 Legal requirements 31
18.5.7 Personal Use 32
18.5.8 SENSITIVE PERSONAL INFORMATION 32
18.5.9 System Monitoring 32
18.5.10 Email accounts 33

18.5.11 Questions 33
18.5.12 Best practices 34
18.5.13 DEFINITIONS 35
18.6 Incident Reporting 38
18.6.1 Introduction 38
18.6.2 What is a non-clinical incident? 38
18.6.3 How should this be reported? 39
18.6.4 How should these be responded to? 40
18.6.5 Follow up 40
18.7 Internet 41
18.7.1 INTRODUCTION 41
18.7.2 OBJECTIVE 41
18.7.3 ORGANISATION RESPONSIBILITIES 42
18.7.4 ACCESS TO THE INTERNET SYSTEM 42
18.7.5 Best practices 42
18.7.6 System Monitoring 43
18.7.7 Questions 43
18.7.8 DEFINITIONS 43
18.8 Remote Access 46
18.8.1 Introduction 46
18.8.2 Purpose of Policy 46
18.8.3 Scope 46
18.8.4 Objectives 46
18.8.5 Principles 46
18.8.6 Responsibilities 47
18.8.7 Risks 47
18.8.8 Security Architecture 48
18.8.9 Security Technologies 48
18.8.10 User Responsibilities, Awareness & Training 49
18.8.11 System Change Control 49
18.8.12 Reporting Security Incidents & Weaknesses 49
18.9 Confidentiality and security of person identifiable Information 50
18.9.1 Introduction 50
18.9.2 Responsibility 50
18.9.3 Scope 51
18.9.4 Disclosure of Information 51
18.9.5 Procedure for Processing a Request For information 51
18.9.6 Security of All Person Identifiable Information 52
18.9.7 Guidance for the transporting of personal and sensitive information 53
18.9.8 Guidance for sharing personal and sensitive information by fax 54
18.9.9 Guidance for sharing personal and sensitive information by phone 55
18.9.10 Guidance for sharing personal and sensitive information by post 56

18.10 Subject Access to Health Records 57
18.10.1 Introduction 57
18.10.2 Scope 57
18.10.3 Responsibility 57
18.10.4 Procedure 57
18.10.5 Requests for urgent computerised records 57
18.10.6 Clients Requests 57
18.10.7 Solicitor Requests 58
18.10.8 Monitoring 58
18.10.9 References 58
18.12 Data Management Policy 59
18.12.1 Statement 59
18.13 Data Protection Policy 60
18.13.1 Introduction 60
18.13.2 Policy 60
18.13.3 Personal Information 61
18.13.4 Basic Principles 61
18.13.5 Duty of Care 61
18.13.6 The role of the information Commissioner's Office 62
18.13.7 Clear Desk Policy 63
18.14 Data Protection & GDPR Policy For Workers, Employees & Consultants 64
18.14.1 Introduction 64
18.14.2 The Six Data Protection Principles 64
18.14.3 Personal Data 65
18.14.4 Special Categories of Personal Data 66
18.14.5 Processing Personal Data 66
18.14.6 When the Clinic Might Process Your Personal Data 67
18.14.7 Sharing Your Personal Data 69
18.14.8 Processing Personal Data for the Clinic 69
18.14.10 Subject Access Requests 70
18.14.11 Data Subjects' Rights 71
18.14.11 Resources 72
18.15 PATIENT INFORMATION LEAFLET – GENERAL DATA PROTECTION REGULATIONS 73
18.16 Records Retention Policy 75
18.17 Computer and Data Security Procedure (Inc. Request to work from home) 81
18.17.1 Introduction 81
18.17.2 Storage and Backup 81
18.17.3 BULK DATA EXTRACTIONS 82
18.17.5 Protection against Viruses 82
18.17.6 Installation of Software 83
18.17.7 HARDWARE 83
18.17.8 Protection against Physical Hazards 83

18.17.9 Protection against Theft or Vandalism via Access to the Building 84
18.17.10 Mobile Computing 85
18.17.12 Home Working 86
18.18 GDPR – Subject Access Request 91
18.18.1 Purpose of the Procedure 91
18.18.2 Background 91
18.18.3 Who should use this procedure 91
18.18.4 Timescales 92
18.19 Clinic Privacy Notice 93
18.19.2 Principles 93
18.19.3 Status 93
18.19.4 Training and support 93
18.19.5 Who it applies to 93
18.19.6 Why and how it applies to them 93
18.19.7 Definition of terms 93
18.19.8 Compliance with regulations 94
18.19.9 Summary 95
18.20 DATA PROTECTION IMPACT ASSESSMENT (DPIA) POLICY 96
18.20.1 Introduction 96
18.20.2 Data Protection Impact Assessment (DPIA) Process 97
18.20.3 When should a DPIA be undertaken? 97
18.20.4 Who Is Required to Complete a DPIA? 98
18.20.5 Applying the Outcome of the Initial Screening Questionnaire ... 98
18.20.6 Roles and Responsibilities 99
18.21 DATA QUALITY POLICY 102
18.21.1 Introduction 102
18.21.2 Purpose and Scope 102
18.21.3 Duties and Responsibilities 102
18.21.4 Definitions 103
18.21.5 Data Quality 103
18.22 INFORMATION SECURITY ASSURANCE POLICY 106
18.22.1 Introduction 106
18.22.3 Securing premises 106
18.22.4 Clear desk and clear screen policy 107
18.22.5 Prevention of unauthorised access 107
18.23 RECORDS MANAGEMENT POLICY 109
18.23.2 Scope 109
18.23.3 Responsibility for Records Management 109
18.23.4 Training 110

18.I NFORMATION GOVERNANCE POLICY

18.1.1 Summary

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

18.1.2 Principles

The clinic recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The clinic fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information. The clinic also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The clinic believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

There are 4 key interlinked strands to the information governance policy:

- Openness
- Legal compliance
- Information security
- Quality assurance

Openness

- Non-confidential information on the clinic and its services should be available to the public through a variety of media, in line with the Clinic code of openness
- The clinic will establish and maintain policies to ensure compliance with the Freedom of Information Act
- The clinic will undertake or commission annual assessments and audits of its policies and arrangements for openness

- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients
- The clinic will have clear procedures and arrangements for liaison with the press and broadcasting media
- The clinic will have clear procedures and arrangements for handling queries from patients and the public

Legal Compliance

- The clinic regards all identifiable personal information relating to patients as confidential
- The clinic will undertake or commission annual assessments and audits of its compliance with legal requirements
- The clinic regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise
- The clinic will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and the common law confidentiality
- The clinic will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act)

Information Security

- The clinic will establish and maintain policies for the effective and secure management of its information assets and resources
- The clinic will undertake or commission annual assessments and audits of its information and IT security arrangements
- The clinic will promote effective confidentiality and security practice to its staff through policies, procedures and training
- The clinic will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security

Information Quality Assurance

- The clinic will establish and maintain policies and procedures for information quality assurance and the effective management of records
- The clinic will undertake or commission annual assessments and audits of its information quality and records management arrangements
- Managers are expected to take ownership of, and seek t
- Improve, the quality of information within their services

- Wherever possible, information quality should be assured at the point of collection
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- The clinic will promote information quality and effective records management through policies, procedures/user manuals and training

18.1.3 Responsibilities

It is the role of the clinic to define the clinic policy in respect of Information Governance, taking into account legal. The clinic is responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

The Information Governance Board is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance in the clinic and raising awareness of Information Governance.

Managers within the clinic are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

18.2 Information Security

18.2.1 Introduction

The purpose of this policy is to recognise the security threats to information systems and to provide a framework for reducing the likelihood of security incidents. It provides high level guidance on ensuring the confidentiality, integrity and availability of information held in electronic format. Specific procedures flowing from the guidance will be implemented locally by each constituent organisation.

Data stored in computer systems represents an increasingly valuable asset to the organisation as systems proliferate and increased reliance is placed upon them. The clinic is committed to protecting its information, and meeting the requirements of doing this.

18.2.2 Objectives, Aim and Scope

Objectives

The objectives of the Policy are to ensure that:

- Information is protected from unauthorised access, disclosure, modification or loss
- Information is authentic
- Information and related equipment are protected from accidental or malicious damage
- Security risks are properly identified, assessed, recorded and managed
- Safeguards to reduce risks are implemented at an acceptable cost
- Audit records on the use of information are created and maintained as necessary
- All legal, regulatory and contractual requirements and standards of due care are met.

The objectives of Brigstock Skin and Laser Information Security Policy are to preserve:

> **Confidentiality** - Access to Data must be confined to those with specific authority to view the data.
> **Integrity** – Information is to be complete and accurate. All systems, assets and networks must operate correctly, according to specification.
> **Availability** - Information must be available and delivered to the right person, at the time when it is needed.

Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Brigstock Skin and Laser by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principals of security and explaining how they will be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

Scope
The Policy applies to all information on electronic systems, which is owned, held in the custody of, or used by the clinic. It applies to all resources used in creating, processing, transmitting, storing, using or controlling that information.

This Security Policy will ensure a consistent approach to the implementation of appropriate security controls against common threats.

The policy shall apply to all members of staff employed by the clinic; furthermore, any external agencies/contractors with access to the clinic network information systems are also subject to this policy.

The requirements of the Policy shall be implemented by the whole of the clinic.

18.2.3 Responsibilities for Security

- Ultimate responsibility for security rests with the Clinic Responsible Individual, but on a day-to-day basis the Registered Manager will be responsible for managing and implementing the policy and related procedures.
- Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:-
    - The information security policies applicable in their work areas
    - Their personal responsibilities for information security
    - How to access advice on information security matters
- All staff must comply with security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.
- Line managers shall be individually responsible for the security of their physical environments.
- Each user shall be responsible for the operational security of the information systems they use.
- Each system user must comply with the security requirements that are currently in force, and must also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

- Contracts with external contractors that allow access the organisation's information systems will be in operation before access is allowed. These contracts will ensure that the staff or sub-contractors of the external organisation will comply with all appropriate security policies.

18.2.4 Legislation

Brigstock Skin and Laser Centre is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation will be devolved to employees and agents of Brigstock Skin and Laser Centre who may be held personally accountable for any breaches of security for which they may be held responsible. Brigstock Skin and Laser Centre will comply with the following legislation and other legislation as appropriate:

The Data Protection Act (1998)
The Copyright, Designs and Patents Act (1988)
The Computer Misuse Act (1990)
The Health and Safety at Work Act (1974)
Human Rights Act (1998)
Regulation of Investigatory Powers Act 2000
Freedom of Information Act 2000
Health & Social Care Act 2000

18.2.5 Policy Framework

Management of Security

- The Clinic Responsible Individual will be responsibility for Information Security.
- The Clinic Registered Manager will be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

Information Security Awareness Training

- The Registered manager will deliver training.
- Information security awareness training will be included in the staff induction process.
- An ongoing awareness programme will be established in order to ensure that staff awareness is refreshed and updated as necessary.

Contracts of Employment

- Security requirements will be addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause.
- Security Requirements will be included in job definitions.

Security Control of Assets

Every asset, (hardware, software, application or data) will have a named custodian who will be responsible for the security of that asset.

18.2.6 Access Controls
Only authorised personnel who have a business need will be given access to restricted areas containing information systems.

18.2.7 User Access Controls
Access to information will be restricted to authorised users who have a business need to access the information.

18.2.8 Computer Access Control
Access to computer facilities will be restricted to authorised users who have a business need to use the facilities.

18.2.9 Application Access Control
Access to data, system utilities and program source libraries will be controlled and restricted to authorised users who have a business need to use the applications. Authorisation to use an application will depend on the availability of a licence from the supplier.

18.2.10 Equipment Security
In order to minimise loss of, or damage to, all assets, equipment will be physically protected from security threats and environmental hazards.

18.2.11 Computer and Network Procedures
Management of computers and networks will be controlled by standard procedures that have been authorised by the Information Governance team.

18.2.12 Security Incidents and weaknesses
All security incidents and weaknesses are to be reported to the Registered Manager. All security incidents will be investigated to establish their cause, operational impact, and business outcome.

18.2.13 Protection from Malicious Software
The organisation will use software counter measures and management procedures to protect itself against the threat of malicious software. All staff will be expected to co-operate fully with this policy. Users must not install software on the organisation's property without permission from the Registered Manager. Users breaching this requirement may be subject to disciplinary action.

18.2.14 User Disks
Disks containing software or data from external sources, or that have been used in external equipment, must be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

18.2.15 Monitoring System Access and Use

An audit trail of system access and use will be maintained and reviewed on a regular basis.

18.2.16 Accreditation of Information Systems

The organisation will ensure that all new information systems, applications and networks include a security plan and are approved by the Information Governance Team before they commence operation.

18.2.17 System Change Control

Changes to information systems, applications or networks must be reviewed and approved by the Governance Team.

18.2.18 Intellectual Property Rights

The organisation will ensure that all information products are properly licensed and approved by the Registered Manager. Users must not install software on the organisation's property without permission from the Registered Manager. Users breaching this requirement may be subject to disciplinary action.

18.2.19 Business Continuity and Disaster Recovery Plans

The organisation will ensure that business continuity and disaster recovery plans are produced for all critical information, applications, systems and networks.

18.2.20 Reporting

The Security Officer will keep the Responsible Individual informed of the information security status of the organisation by means of regular reports.

18.2.21 Policy Audit

This policy will be subject to audit by the registered manager

18.2.22 Further Information

Further information and advice on this policy can be obtained from the Registered Manager.

18.2.23 Do's and Don'ts for Users"

Do……

Do understand that Information Security is EVERYONE'S responsibility including YOU!

Do Ensure that you and any member of the clinic for whom you are responsible has signed the Compliance Agreement

Do Report immediately any threat to, or suspected breach of information security to the Registered Manager.
Do consult the clinic registered manager in any case of doubt
Do Ensure that the IT equipment for which you are responsible is kept and

operated in a secure manner
Do Ensure that all visitors are escorted and supervised
Do Ensure that any floppy disc, USB sticks, CDs or other magnetic media is virus checked before use
Do Ensure that you save your work on the clinic software.
Do Store floppy discs securely
Do Keep your password(s) secure and do not disclose to any other team member
Do Log-out of your work station when leaving your desk
Do Dispose of printouts containing any form of sensitive data securely (eg. by shredding or through the confidential waste disposal system operated by the clinic)
Do regularly clear out your mailbox and unused files from your mail box account

Don't …

Don't assume that someone else has taken responsibility for a threat or breach of security. Responsibility lies with the whole Clinic.

Don't Leave visitors unattended with access to a logged on screen
Don't Load software that has not been virus checked
Don't change your default display settings
Don't Forget to make backup copies of data held on the C Drive
Don't Throw away discs unless they have been reformatted or broken
Don't Attach a modem
Don't Reveal your password
Don't Leave your terminal logged on when you leave your desk
Don't Share sensitive information with anyone not specifically authorised to receive it.
Don't copy application software unless specifically tasked to do so by the Systems Administrator

18.3 Network Security

18.3.1 Introduction

This document defines the Network Security Policy for Brigstock Skin and Laser. The Network Security Policy applies to all business functions and information contained on the network, the physical environment and relevant people who support the network. This document **s**ets out the organisation's policy for the protection of the confidentiality, integrity and availability of the network. It establishes the security responsibilities for network security and provides reference to documentation relevant to this policy.

18.3.2 Aim

- The aim of this policy is to ensure the security of Brigstock Skin and Laser's network. To do this the Trust will:
- Ensure Availability
- Ensure that the network is for users.
- Preserve Integrity
- Protect the network from unauthorised or accidental modification ensuring the accuracy and completeness of the organisation's assets.
- Preserve Confidentiality
- Protect assets against unauthorised disclosure.

18.3.3 Network definition

The network is a collection of communication equipment such as servers, computers, printers, and modems, which has been connected together by cables. The network is created to share data, software, and peripherals such as printers, modems, fax machines, Internet connections, CD-ROM and tape drives, hard disks and other data storage equipment.

18.3.4 Scope of this Policy

This policy applies to all networks within Brigstock Skin and Laser used for:

- The storage, sharing and transmission of non-clinical data and images
- The storage, sharing and transmission of clinical data and images
- Printing or scanning non-clinical or clinical data or images
- The provision of Internet systems for receiving, sending and storing non-clinical or clinical data or images

18.3.5 The Policy

The overall Network Security Policy for Brigstock Skin and Laser is described below:

The Brigstock Skin and Laser information network will be available when needed, can be accessed only by legitimate users and will contain complete

and accurate information. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this, Brigstock Skin and Laser will undertake the following:

- Protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.
- Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
- Implement the Network Security Policy in a consistent, timely and cost effective manner.
- Where relevant, Brigstock Skin and Laser Centre will comply with:

Copyright, Designs & Patents Act 1988
Access to Health Records Act 1990
Computer Misuse Act 1990
The Data Protection Act 1998
The Human Rights Act 1998
Electronic Communications Act 2000
Regulation of Investigatory Powers Act 2000
Freedom of Information Act 2000
Health & Social Care Act 2001

Brigstock Skin and Laser will comply with other laws and legislation as appropriate. The policy must be approved by the Information Security Manager (ISM) or Registered Manager.

18.3.6 Risk Assessment

- Brigstock Skin and Laser will carry out security risk assessment(s) in relation to all the business processes covered by this policy. These risk assessments will cover all aspects of the network that are used to support those business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.
- Risk assessment will be conducted to determine the ITSEC Assurance levels required for security barriers that protect the network.
- Formal risk assessments will be conducted using a risk assessment process and will conform to ISO17799.

18.3.7 Physical & Environmental Security

- Network computer equipment will be housed in a controlled and secure environment. Critical or sensitive network equipment will be housed in an environment that is monitored for temperature, humidity and power supply quality.

- Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.
- The Registered Manager is responsible for ensuring that door lock codes are changed periodically, following a compromise of the code, if s/he suspects the code has been compromised, or when required to do so by the Information Security Manager (ISM) or Information Security Officer (ISO).
- Critical or sensitive network equipment will be protected from power supply failures.
- Critical or sensitive network equipment will be protected by intruder alarms and fire suppression systems.
- Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.
- All visitors to secure network areas must be authorised by the Registered Manager.
- All visitors to secure network areas must be made aware of network security requirements.
- All visitors to secure network areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out.
- All visitors to secure network areas must be provided with a visitors ID badge, which should be worn while they are on the premises.
- The Registered Manager will ensure that all relevant staff are made aware of procedures for visitors and that visitors are escorted, when necessary.

18.3.8 Access Control to Secure Network Areas

Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it. The Registered Manager will maintain and periodically review a list of those with unsupervised access.

18.3.9 Access Control to the Network

- Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Remote access to the network will conform to the clinic Remote Access Policy.
- There must be a formal, documented user registration and de-registration procedure for access to the network.
- The Registered Manager must approve user access.
- Access rights to the network will be allocated on the requirements of the user's job, rather than on a status basis.
- Security privileges (i.e. 'superuser' or network administrator rights) to the network will be allocated on the requirements of the user's job, rather than on a status basis.
- Access will not be granted until the Registered Manager registers a user.
- All users to the network will have their own individual user log in, identification and password.

- Users are responsible for ensuring their password is kept secret (see User Responsibilities).
- User access rights will be immediately removed or reviewed for those users who have left the clinic or changed jobs.

18.3.10 Third Party Access Control to the Network

Third party access to the network will be based on a formal contract that satisfies all necessary security conditions. All third party access to the network must be logged.

18.3.11 External Network Connections

- Ensure that all connections to external networks and systems have documented and approved System Security Policies.
- Ensure that all connections to external networks and systems conform to the Network Security Policy, Code of Connection and supporting guidance.
- The ISO or Registered Manager should approve all connections to external networks and systems before they commence operation.

18.3.12 Maintenance Contracts

The Registered Manager will ensure that maintenance contracts are maintained and periodically reviewed for all network equipments. All contract details will constitute part of the Information Clinic Asset register.

18.3.13 Data and Software Exchange

Formal agreements for the exchange of data and software between organisations must be established and approved by the Registered Manager.

18.3.14 Fault Logging

The Network Manager or Registered Manager is responsible for ensuring that a log of all faults on the network is maintained and reviewed. A written procedure to report faults and review countermeasures will be produced.

18.3.15 Security Operating Procedures (SyOps)

Produce Security Operating Procedures (SyOps) and security contingency plans that reflect the Network Security Policy. Changes to operating procedures must be authorised by the Registered Manager.

18.3.16 Network Operating Procedures

- Documented operating procedures should be prepared for the operation of the network, to ensure its correct, secure operation.
- Changes to operating procedures must be authorised by the Registered Manager.

18.3.17 Data Backup and Restoration

- The Registered Manager is responsible for ensuring that backup copies of network configuration data are taken regularly.
- Documented procedures for the backup process and storage of backup tapes will be produced and communicated to all the relevant staff.
- All backup tapes will be stored securely and a copy will be stored off-site.
- Documented procedures for the safe and secure disposal of backup media will be produced and communicated to all relevant staff.
- Users are responsible for ensuring that they backup their own data to the network server.

18.3.18 User Responsibilities, Awareness & Training

- The Clinic will ensure that all users of the network are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities.
- All users of the network must be made aware of the contents and implications of the Network Security Policy and SyOps.
- Irresponsible or improper actions by users may result in disciplinary action(s).

18.3.19 Accreditation of Network Systems

Ensure that the network is approved by the Registered Manager before it commences operation. The Registered Manager is responsible for ensuring that the network does not pose an unacceptable security risk to the organisation.

18.3.20 Security Audits

The Registered Manager will require checks on, or an audit of, actual implementations based on approved security policies.

18.3.21 Malicious Software

Ensure that measures are in place to detect and protect the network from viruses and other malicious software.

18.3.22 Secure Disposal or Re-use of Equipment

- Ensure that where equipment is being disposed of, IT Department staff must ensure that all data on the equipment (e.g. on hard disks or tapes) is securely overwritten. Where this is not possible IT Department staff should physically destroy the disk or tape.

- Ensure that where disks are to be removed from the premises for repair, where possible, the data is securely overwritten or the equipment de-gaussed by the IT Department.

18.3.23 System Change Control

Ensure that the relevant Registered Manager reviews changes to the security of the network. All such changes must be reviewed and approved by the Registered Manager. The Network Managers are responsible for updating all relevant Network Security Policies, design documentation, security operating procedures and network operating procedures.

- The Registered Manager may require checks on, or an assessment of the actual implementation based on the proposed changes.

- The Registered Manager is responsible for ensuring that selected hardware or software meets agreed security standards.

- As part of acceptance testing of all new network systems, the Registered Manager will attempt to cause a security failure and document other criteria against which tests will be undertaken prior to formal acceptance.

- Testing facilities will be used for all new network systems. Development and operational facilities will be separated.

18.3.24 Security Monitoring

Ensure that the network is monitored for potential security breaches. All monitoring will comply with current legislation.

18.3.25 Reporting Security Incidents & Weaknesses

All potential security breaches must be investigated and reported to the Registered Manager. Security incidents and weaknesses must be reported in accordance with the requirements of the organisation's incident reporting procedure.

18.3.26 System Configuration Management

Ensure that there is an effective configuration management system for the network.

18.3.27 Business Continuity & Disaster Recovery Plans

Ensure that business continuity plans and disaster recovery plans are produced for the network. The plans must be reviewed by the Registered Manager and tested on a regular basis.

18.3.28 Unattended Equipment and Clear Screen

- Users must ensure that they protect the network from unauthorised access. They must log off the network at the end of their shift.
- The Trust operates a clear screen policy that means that users must ensure that any equipment logged on to the network must be protected if they leave it unattended, even for a short time. Workstations must be

locked or a screensaver password activated if a workstation is left unattended for a short time.
- Users failing to comply will be subject to disciplinary action.

18.3.29 Security Responsibilities

The Clinics Responsible Individual has delegated the overall security responsibility for security, policy and implementation to the Registered Manager. Responsibility for implementing this policy within the context of IT systems development and use in the organisation is delegated further to the ISO or the Registered Manager.

18.3.30 Registered Manager's Responsibilities

- To produce and implementing effective security countermeasures.
- Produce all relevant security documentation, security operating procedures and contingency plans reflecting the requirements of the Network Security Policy.
- All such documentation will be included in the Information Department's Asset register.
- Acting as a central point of contact on information security within the organisation, for both staff and external organisations.
- Implementing an effective framework for the management of security.
- Assisting in the formulation of Information Security Policy and related policies.
- Advise on the content and implementation of the Information Security Programme.
- Produce organisational standards, procedures and guidance on Information Security matters for approval by the Information Governance Steering Group.
- Co-ordinate information security activities particularly those related to shared information systems or IT infrastructures.
- Liaise with external organisations on information security matters, including representing the organisation on cross-community committees.
- Ensuring that appropriate Data Protection Act notifications are maintained for information stored on the network.
- Dealing with enquires, from any source, in relation to the Data Protection Act and facilitating Subject Access Requests.
- Advising users of information systems, applications and networks of their responsibilities under the Data Protection Act, including Subject Access.
- Advising the clinic on breaches of the Act and recommended actions.
- Encouraging, monitoring and checking compliance with the Data Protection Act.
- Liaising with external organisations regarding Data Protection Act matters.
- Promoting awareness and providing guidance and advice related to the Data Protection Act as it applies within the Clinic.

18.3.31 Registered Manager's Responsibilities

- Reporting Information to the Responsible Individual on matters relating to IT security.
- Creating, maintaining, giving guidance on and overseeing the implementation of IT Security.
- Representing the organisation on internal and external committees that relate to IT security.
- Ensuring that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk.
- Ensuring the systems, application and/or development of required policy standards and procedures in accordance with needs, policy and guidance set centrally by the Information Security Manager.
- Ensuring that access to the organisation's network is limited to those who do not have the necessary authority and clearance.
- Providing advice and guidance to develop teams to ensure that the policy is complied with.
- Approving system security policies for the infrastructure and common services.
- Approving tested systems and agreeing rollout plans.
- Advising the Information Security Manager on the accreditation of IT systems, applications and networks.
- Providing a central point of contact on IT security issues.
- Providing advice and guidance on:
    - Policy Compliance
    - Incident Investigation
    - IT Security Awareness
    - IT Security Training
    - IT Systems Accreditation
    - Security of External Service Provision
    - Contingency Planning for IT systems
- Contacting the Information Security Manager when:
    - Incidents or alerts have been reported that may affect the organisation's systems, applications or networks.
    - Proposals have been made to connect the organisation's systems, applications or networks to systems that are operated by external organisations.
    - Passing on the advice of external sources/authorities on IT security matters.

18.3.32 Line Manager's Responsibilities

- Ensuring the security of the network, that is information, hardware and software used by staff and, where appropriate,

by third parties is consistent with legal and management requirements and obligations.
- Ensuring that their staff are made aware of their security responsibilities.
- Ensuring that their staff receives suitable security training.

18.3.33 General Responsibilities

All personnel or agents acting for the organisation have a duty to:

- Safeguard hardware, software and information in their care.
- Prevent the introduction of malicious software on the organisation's IT systems.
- Report on any suspected or actual breaches in security.

18.4 User Access Management

18.4.1 Introduction

The purpose of this policy is to prevent unauthorized access to Brigstock Skin and Laser information systems. The policy describes the registration and de-registration process for all clinic information systems and services.

This policy applies especially to new starters, leavers and those moving job, responsibility or Portfolio.

This policy should also be seen in the light of HR procedures to verify new starter's qualifications, references and right to work in this country.

18.4.2 User registration

New Users

Access to the clinic information services is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager.

Each user is identified by a unique user ID so that users can be linked to make responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out (i.e. Training).

There is a standard level of access to the clinic software, all other services can be accessed when specifically authorised by HR/line management.

A request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR. The request is free format, but must state:

- Name of person making request
- Job title of the newcomers and workgroup
- Start date
- Services required (default services are: MS Outlook, MS Office and Internet access)

Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure.

The user signs the form indicating that they understand the conditions of access.

Access to all Clinic systems is provided by IT and can only be started after proper procedures are completed.

A new user will be set up on receipt of written notification but not made available, by issue of password, until the individual's start date.

Clinic Software will maintain a record of all requests in a folder named "new users" in the Helpdesk, National mailbox and will file email paper copies in the user access file.

18.4.3 Change of user requirements

Changed requirements will normally relate to an alteration to the applications used but may also involve network access. Requests must be in writing (e-mail or hard copy) and must be directed to the line manager.

Changes will be made on receipt of a properly completed request, the same details as shown above are required and requests will be filed under "access change requests" in the Helpdesk, National mailbox.

The Information Security Officer (ISO) will not normally be copied in on requests but must be consulted if the request is not for a standard network service.

18.4.4 Change of password

Where a user has forgotten his/her password, the user should follow the necessary instruction, set by Clinic Software to obtain a new one.

18.4.5 Removal of users

As soon as an individual leaves the Clinic employment, all his/her system logons must be revoked.

As part of the employee termination process HR (or line managers in the case of contractors) will inform IT operations of all leavers and their date of leaving.

All notification will be filed in a folder called "Leavers" in the Helpdesk, National mailbox.

Additionally, IT operations will positively confirm leavers with HR, each Friday, retaining a copy of the e-mail and reply in a file "Leavers" in the Helpdesk, National mailbox, or hard copy in the user access file.

Unless otherwise advised, IT operations will delete network access for all leavers at 4pm each Friday (or on the leaving date if not a Friday) (old user ID's are removed and not re-issued). This will include access to all network services. IT operations will inform application owners of leavers where their systems are affected.

The clinic expects all leavers to hand over current files within their workgroup; however IT operations can move a leavers files to specific areas if requested. Normally a leaver's data will be left in its existing directory for one month and then archived off system (but can be recovered if required).

18.4.6 Privilege management

"Special privileges" are those allowed to use the clinic manager or systems programmers, allowing access to sensitive area (for example, passwords). The unnecessary allocation and use of special privileges is often found to be a major contributing factor to the vulnerability of systems that have been breached

Privileged access must be authorised by the Registered Manager, using the request form shown in Appendix 46. All completed forms, both current and expired, will be held by the ISO who is authorised by the completed form to set up the access specified.

All requests for access outside normal services must be supported by a completed and authorised Privilege Access form.

The Registered Manager will maintain a master list of privileged accesses, which are in use, and this will be checked and confirmed by the ISO on a three monthly basis. The list will identify all separate logons for each system and service.

18.4.7 User password management

Password format and general rules are held within the Information Security – A Guide to Staff. Systems logon requires that all passwords be of a minimum of 7 characters.

Temporary access may be granted on a need to use basis. Such logons may be granted by the ISO) but must be recorded and reported on the normal form. Temporary logons must be identified by a specific login (starting TEMP****) and must be deleted immediately after use.

Temporary access may be granted on a need to use basis. Such logons may be granted by the ISO but must be recorded and reported on the normal form.

Temporary logons must be identified by a specific login (starting TEMP****) and must be deleted immediately after use.

18.4.8 Review of user access rights

The ISO will institute a review of all network access rights at least twice a year, which is designed to positively confirm all users.

Any lapsed or unwanted logons, which are identified, will be disabled immediately and will be deleted unless positively reconfirmed.

Annually, the ISO will institute a review of access to applications. This will be done in cooperation with the application owner and will be designed to positively re-confirm all users. All other logons will be deleted.

The review will be conducted as follows.

- The ISO will generate a list of users, by application.
- The appropriate list will be sent to each Application owner who will be asked to confirm that all users identified are authorised to use the system.
- The ISO will ensure a response.
- Any user not confirmed will have his/her access to the system removed.
- The ISO will maintain a file of -
    - Lists sent over
    - Application owner responses
    - A record of action taken
- The review will normally be conducted on an annual basis

18.5 Computer Internet and Email Usage

Introduction

18.5.1

- The clinic's computers and IT network are invaluable resources which must be used appropriately
- The internet offers access to almost infinite sources of information
- Email offers a fast, inexpensive and convenient way to communicate both inside and outside the Clinic
- The Clinic wishes to ensure that these resources are used responsibly and productively

18.5.2 APPLICABILITY

The policy applies to all employees and Partners, and also applies to other people who work at the clinic e.g. self-employed staff, temporary staff and contractors and who have access to the clinic computer systems.

18.5.3 THE POLICY

a) Access to and use of computers

- You must keep confidential your username/password and must not divulge these to anyone. A lost or forgotten username or password must be reported to the line manager.
- If you think your username/password may be known to someone else, notify your line manager immediately.
- It is illegal under the Computer Misuse Act ('the Act') to steal or guess someone's username/password and to use this information to access, modify or delete data which you are not authorised to access, or to alter settings on a computer or otherwise affect its operation. It is also an offence under the Act to use someone's username/password to access a computer through which to commit other illegal acts such as 'hacking' into someone's bank account and stealing funds. Offences under the Act carry penalties of imprisonment and/or a fine.
- If you are suspected of any such offences the clinics's Disciplinary Procedure will be invoked. If after investigation and it becomes apparent that you have offended under terms of the Act, prosecutions may be brought

b) The internet

- All staff have access to the internet
- Internet access to be solely for business use
- You must not create personal web pages or web logs (‘blogs’) using clinic time and resources
- You must not visit social networking websites such as (but not limited to) Facebook, MySpace, Bebo, Twitter, YouTube.
- You must not surf for or download unsuitable (especially pornographic) material
- Suitable anti-spyware, adware, anti-phishing, worm, trojan and any other appropriate protection software must be kept up to date and not circumvented
- You must not engage in activities of questionable legality (e.g. gambling)
- The registered manager/nurse manager/admin team will keep the Clinic website updated
- Any material downloaded from the internet must be checked for viruses
- Any copyright, licence or usage terms on material or software downloaded from the internet must be observed
- Any licence or usage fees due on material or software downloaded from the internet must be paid (prior authorisation for the expenditure must be obtained)
- The Clinic must not be committed to any purchases over the internet unless authorised by a manager
- Secure transactions must be used for any purchases over the internet
- Internet usage may be monitored to ensure compliance with the Policy
- Penalties for mis-use include withdrawal of access and if necessary the implementation of the appropriate policy for Harassment or Discrimination offences or the Clinics Disciplinary Procedure
- If, in your own time, you create your own blog or place information on social networking sites, You Tube, or any other publically available location on the internet, it will be a disciplinary matter if you make any direct or indirect reference to the Clinic or your employment at the Clinic.

c) Email

- All staff have access to email
- Usage of external email (i.e. email over the internet) to be solely for working purposes
- Incoming emails and any attachments must be checked for viruses/automatic virus checking must not be circumvented. Anti virus software must be kept up to date
- Emails (both internal and external) must not contain unsuitable information or attachments e.g. defamatory/discriminatory/bullying/harassing material or comments
- All emails sent externally must include a standard disclaimer (an example is shown below)

- Any confidential information (especially clients identifiable information) sent in an email must be encrypted
- You must not reveal or publicise confidential or proprietary information about the clinic.
- You must not represent personal opinions as those of the clinic
- Care must be taken in addressing emails (especially when using 'copies to', address books and distribution lists) to ensure that emails are sent only to the intended recipients.
- You must not access, change, or use another person's username/password/email account or files for which you do not have explicit authorisation. If you are asked to check someone else's email (e.g. when that person is on holiday or off sick), this must be authorised by your line manager.
- Email usage and content may be monitored to ensure compliance with the Policy
- Penalties for mis-use include withdrawal of access and if necessary the implementation of the appropriate policy for Harassment or Discrimination or the Clinics Disciplinary Procedure.

18.5.5 Email disclaimer

The following disclaimer must be appended to every external email sent from the Clinic.

E-MAIL DISCLAIMER - IMPORTANT INFORMATION

The contents of this e-mail are confidential and protected by copyright. The email is intended for the named addressee only. If you are not the named addressee (or a person acting on behalf of and with the authority of the addressee) and have received this e-mail by mistake any copying, disclosure or dissemination of the contents of this e-mail to any third party is strictly forbidden by the sender. If you have received this e-mail in error, please contact the sender immediately by return of e-mail and then delete this e-mail and destroy any copies thereof. Please also note that Brigstock Skin and Laser endeavours at all times to keep its network free of viruses. You should, however, scan this e-mail and any attachments to it for any viruses. Brigstock Skin and Laser will not be held responsible for any viruses which may be transmitted upon receipt of this e-mail or the opening of any attachment thereto. Unless otherwise stated, any views or opinions presented are solely those of the author and do not necessarily represent those of Brigstock Skin and Laser Emails may be monitored.

18.5.6 Legal requirements

The following rules are required by law and are to be strictly adhered to:

- It is strictly prohibited to send or forward emails containing libellous, defamatory, offensive, harassing, racist, obscene or pornographic remarks or depictions. If you receive an email of this nature, you must promptly notify your supervisor.
- Do not forward a confidential message without acquiring permission from the sender first.
- Do not send unsolicited email messages.
- Do not forge or attempt to forge email messages.
- Do not send email messages using another person's email account.
- Do not breach copyright or licensing laws when composing or forwarding emails and email attachments.

18.5.7 Personal Use

Although the Organisation's email system is meant for business use, the Organisation allows the reasonable use of email for personal use if certain guidelines are adhered to:

- Personal use of email should not interfere with work.
- Personal emails must also adhere to the guidelines in this policy.
- Personal emails are kept in a separate folder, named 'Private'. The emails in this folder must be deleted weekly so as not to clog up the system.
- The forwarding of chain letters, junk mail, jokes and executables is strictly forbidden.

18.5.8 SENSITIVE PERSONAL INFORMATION

- Email is an insecure system. Therefore, sensitive personal information (i.e. that relating to identifiable individuals) or commercially sensitive information MUST NOT be sent by email unless it is encrypted using software approved by the Organisation.

18.5.9 System Monitoring

- All emails are monitored for viruses. All email traffic (incoming and outgoing) is logged automatically. The logs do not include email content. These logs are audited periodically.
- The content of emails is not routinely monitored. However, the Organisation reserves the right to retain message content as required to meet legal and statutory obligations.
- If there is evidence that you are not adhering to the guidelines set out in this policy, the Organisation reserves the right to take disciplinary action, which may lead to a termination of contract and/or legal action.

18.5.10 Email accounts

All email accounts maintained on our email systems are property of the Organisation.

18.5.11 Questions

If you have any questions or comments about this Email Policy, please contact the registered manager. If you do not have any questions, the Organisation presumes that you understand and are aware of the requirements of the Email Policy and will adhere to them.

18.5.12 Best practices

The Organisation considers email as an important means of communication and recognises the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service.

Therefore the Organisation wishes users to adhere to the following guidelines:

- Write well-structured emails and use short, descriptive subjects.
- The Organisation's email style is informal. This means that sentences can be short and to the point. You can start your email with 'Hi', or 'Dear', and the name of the person. Messages can be ended with 'Best Regards'. The use of abbreviations and characters such as smileys however, is not encouraged.
- Signatures must include your name, job title and Organisation name.
- Use the spell checker before you send out an email.
- Do not send unnecessary attachments.
- Do not write emails in capitals. This appears as if you are shouting and is considered rude.
- Do not print emails unless you really need to for work purposes. Emails can be saved, if you need them.
- If you need a reply to your email by a particular date let the recipient know this.
- If you forward mails, state clearly what action you expect the recipient to take.
- Only send emails the content of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, using other means of communication, or protecting information by using a password.
- Only mark emails as important if they really are important.
- Ensure you send your email only to people who **need** to see it. Sending emails to all in your address book can unnecessarily block the system.
- Emails should be treated like any other correspondence and should be answered as quickly as possible.
- Delete any email messages that you do not need to have a copy of.
- If you suspect you received a virus by email telephone the IT Helpdesk immediately.
- Do not switch off your PC unless told to do so by the IT Helpdesk.
- Do not attempt to remove the virus yourself. The Helpdesk will need to know what virus it is.

18.5.13 DEFINITIONS

1. Defamation & libel

What is defamation & libel?
A published (spoken or written) statement or series or statements that affects the reputation of a person (a person can be a human being or an organisation) and exposes them to hatred, contempt, ridicule, being shunned or avoided, discredited in their trade, business, office or profession, or pecuniary loss. If the statement is not true then it is considered slanderous or libellous and the person towards whom it is made has redress in law.

What you must not do
Make statements about people or organisations in any email that you write without verifying their basis in fact. Note that forwarding an email with a slanderous or libellous statement also makes you liable.

What are the consequences of not following this policy?
You and the Organisation may be subject to expensive legal action.

2. Harassment
What is harassment?
Words, conduct or action, usually repeated or persistent that, being directed at a specific person, annoys, alarms, or causes substantial emotional distress in that person and serves no purpose.

What you must not do
Use the email system to harass other members of staff by sending or forwarding messages that they consider offensive or threatening.

What are the consequences of not following this policy?
The Organisation deals with harassment by providing advice, support and mediation. Those perpetrating harassment can also be made subject to the Organisation's Disciplinary procedure. *Any proven case of harassment will result in disciplinary action against the guilty party which could ultimately lead to their dismissal.*

3. Pornography

What is pornography?

Pornography can take many forms. For example, textual descriptions still and moving images, cartoons and sound files. Some pornography is illegal in the UK and some is legal. Pornography considered legal in the UK may be illegal elsewhere. Because of the global nature of email these issues must be taken into consideration. Therefore, the Organisation defines pornography as the description or depiction of sexual acts or naked people that are designed to be sexually exciting. The Organisation will not tolerate its facilities being used for this type of material and considers such behaviour to constitute a serious disciplinary offence.

What you must not do

- Send or forward emails containing pornography. If you receive an email containing pornography you should report it to the registered manager or your supervisor.
- Send or forward emails with attachments containing pornography. If you receive an email with an attachment containing pornography you should report it to the registered manager or your supervisor.
- Save pornographic material that has been transmitted to you by email.

What are the consequences of not following this policy?

- Users and/or the Organisation can be prosecuted or held liable for transmitting pornographic material in the UK and elsewhere.
- The reputation of the Organisation will be seriously questioned if pornographic material has been transmitted and this becomes publicly known.
- Users found to be in possession of pornographic material, or to have transmitted pornographic material, may be subject to Organisation disciplinary action.

4. Copyright

What is copyright?

Copyright is a term used to describe the rights under law that people have to protect original work they have created. The original work can be a computer program, document, graphic, film or sound recording, for example. Copyright protects the work to ensure no one else can copy, alter or use the work without the express permission of the owner. Copyright is sometimes indicated in a piece of work by this symbol ©. However, it does not have to be displayed under British law. So a lack of the symbol does not indicate a lack of copyright. In the case of computer software, users purchase a licence to use the work. The Organisation purchases licences on behalf of its users.

What you must not do

- Alter any software programs, graphics etc without the express permission of the owner.
- Claim someone else's work is your own
- Send copyrighted material by email without the permission of the owner. This is considered copying.

What are the consequences of not following this policy?

- A user and/or the Organisation can face fines and/or up to two years imprisonment for infringing copyright.

18.6 Incident Reporting

18.6.1 Introduction

The clinic has a responsibility to monitor all non-clinical incidents that occur within the organisation that may breach security and/or confidentiality of personal information. The clinic also needs to ensure that all incidents are identified, reported, monitored. The clinic already has a method of recording clinical incidents but not necessarily non-clinical incidents relating to breaches of security and confidentiality.

The document attempts to detail the process of identifying, recording and monitoring non-clinical incidents. This is a requirement of the Caldicott recommendations and ISO27001/ISO27002/BS7799, the Information security management standard.

18.6.2 What is a non-clinical incident?

A non-clinical incident relating to breaches of security and/or confidentiality could be anything from users of computer systems sharing passwords to a piece of paper identifying a client being found in the high street.

A security incident might be a ‘usual’ everyday event e.g. accidentally entering the wrong password or the wrong user id, forgetting to change a password within a specified time period.

A security incident might be an ‘unusual’ event e.g. something odd happening on the screen, a computer file disappearing, an unaccompanied stranger in a restricted area.

An IM&T security incident is defined as any event that has resulted or could result in:

- The disclosure of confidential information to any unauthorised person
- The integrity of the system or data being put at risk
- The availability of the system or information being put at risk
- An adverse impact e.g.
    - Embarrassment to the clinic
    - Threat to personal safety or privacy
    - Legal obligation or penalty
    - Financial loss
    - Disruption of activities

All incidents should be reported to the immediate line manager, security officer and Caldicott Guardian.

Some incidents may impact on other parts of the clinic e.g. a virus and if this is the case the incident should be reported to the Registered Manager.

Some examples of these types of incidents include:

- Finding computer printout of clients details at the play group
- Finding a clinic list, the back of which is used for a shopping list, in the supermarket
- Finding a patient manual record in a ladies toilet within a hospital site
- Finding a patient record in the back of an unattended wheelchair used by porters to move patients
- Identifying that a fax that was thought to have been sent to a clinician had been received by a private householder
- Giving out identifiable information about an individual over the telephone
- Losing a laptop computer with personal information on it
- Giving information to someone who should not have access to it – verbally, in writing or electronically
- Accessing a computer database using someone else's authorisation e.g. someone else's user id and password
- Trying to access a secure area using someone else's swipe card or pin number when not authorised to access that area
- Finding your PC and/or programmes aren't working correctly – potentially because you may have a virus
- Software malfunction
- Sending a sensitive e-mail to 'all staff' by mistake
- Finding an employee's password written down on a 'post-it'
- Finding someone has tried to 'break in' to the office/building

18.6.3 How should this be reported?

All employees (contracted and non-contract) should be made aware through their contract of employment, training and by their manager of what is considered to be an incident.

They should be made aware that if they discover something that could be considered as an incident, they should report this to their manager and complete a non-clinical risk incident reporting form (a copy of a 'draft' form is attached for this purpose at appendix 47).

This form should be copied to the Security Officer and the Caldicott Guardian and a copy kept within the department.

The form, which should be numbered, should identify the following:

- Date of discovery of incident
- Place of incident
- Who discovered incident
- Details of incident
- Category/classification of incident
- Report to senior management if risk to organisation and/or patient care

- Any action taken by person discovering incident at time of discovery
- Date incident reporting form has been sent to the security officer and/or Caldicott Guardian
- Action taken by security officer and/or Caldicott Guardian/Group to ensure incident does not occur again
- Follow-up action to check no re-occurrence of incident

18.6.4 How should these be responded to?

Incident reporting forms should be sent to the security officer and the Caldicott Guardian. If there is a Caldicott group or other group looking at security and confidentiality issues the form should also be sent to that group.

The Guardian and/or group should log the incident to enable a central register to be maintained of all incidents occurring within the organisation.

All registered incidents should be re-evaluated after a 6 month period to ensure the type of incident is no longer being reported or the volume of those types of incidents has dramatically reduced.

If there is no change in the volume of each type of incident the senior management should be alerted and appropriate action taken. This could be further training courses for staff or an improvement to existing security and/or confidentiality arrangements.

Some incidents may involve the invoking of the clinic Disciplinary Procedures. Incidents that are deemed to be a disciplinary offence are detailed within the Disciplinary Procedures.

18.6.5 Follow up

Incidents should be used in training sessions about security and confidentiality as using 'real life events' relevant to an organisation can always be related to, by staff, a lot better than imaginary events. This will give attendees an example of what could occur, how to respond to such events and how to avoid them in the future.

18.7 Internet

18.7.1 INTRODUCTION

This document defines the Internet use Policy for Brigstock Skin and Laser Centre. The Internet use Policy applies to all users of the Internet and relevant people who support the Internet system.

The Internet is a general term that covers access to numerous computers and computer systems worldwide that are accessed electronically. Such systems include the World Wide Web (WWW), email (dealt with in a separate policy), File Transfer Protocol (FTP), newsgroups, Gopher, etc.

This document:

- Sets out the Organisation's policy for the protection of the confidentiality, integrity and availability of the Internet system.
- Establishes Organisation and user responsibilities for the Internet system.
- Provides reference to documentation relevant to this policy.

18.7.2 OBJECTIVE

The objective of this policy is to ensure the security of Internet system. To do this the Organisation will:

- Ensure Availability
- Ensure that the Internet system is available for users.
- Preserve Integrity
- Protect the Internet system from unauthorised or accidental modification ensuring the accuracy and completeness of the Organisation's assets.
- Preserve Confidentiality
- Protect assets against unauthorised disclosure.

The purpose of this policy is to ensure the proper use of the Organisation's Internet system and make users aware of what the Organisation deems as acceptable and unacceptable use of its Internet system.
By following the guidelines in this policy, the Internet user can minimise the legal risks involved in the use of Internet. If any user disregards the rules set out in this Internet use Policy, the user will be fully liable and may be subject to disciplinary action by the Clinic.

18.7.3 ORGANISATION RESPONSIBILITIES

- The Organisation will ensure that all users are properly trained before using the Internet system.
- The Organisation will take all reasonable steps to ensure that users of the Internet service are aware of policies, protocols, procedures and legal obligations relating to the use of Internet. This will be done through training and staff communications at departmental and Organisation-wide levels.
- The Organisation will ensure all users of the Internet are registered.

18.7.4 ACCESS TO THE INTERNET SYSTEM

Anyone wishing to open an Internet account must obtain an Internet Access Application Agreement from the IT Department. Complete the agreement and return it to the IT department.

18.7.5 Best practices

The Organisation considers the Internet as an important means of communication and recognises the importance of proper Internet content and speedy replies in conveying a professional image and delivering good customer service. Therefore the Organisation wishes users to adhere to the following guidelines:

Acceptable Internet Usage:

- To access research material and other information relevant to your work.

Unacceptable Internet Usage

- Accessing social networking websites
- Creating, downloading or transmitting (other than for properly authorised and lawful research) any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- Creating, downloading or transmitting (other than for properly authorised and lawful research) any defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material.
- Creating, downloading or transmitting material that is designed to annoy, harass, bully, inconvenience or cause needless anxiety to other people.
- Creating or transmitting “junk-mail” or “spam”. This means unsolicited commercial web mail, chain letters or advertisements.
- Using the Internet to conduct private or freelance business for the purpose of commercial gain.
- Creating, downloading or transmitting data or material that is created for the purpose of corrupting or destroying other user’s data or hardware.
- Downloading streaming video or audio for entertainment purposes.

18.7.6 System Monitoring

All Internet traffic is logged automatically (each site a user visits is included in the log, with the time visited and pages viewed) to ensure that damaging code or viruses do not enter the organisation's network or systems. These logs are audited periodically by the Registered Manager.
If there is evidence that you are not adhering to the guidelines set out in this policy, the Organisation reserves the right to take disciplinary action, which may lead to a termination of contract and/or legal action.

18.7.7 Questions

If you have any questions or comments about this Internet use Policy, please contact the Registered Manager. If you do not have any questions the Organisation presumes that you understand and are aware of the rules and guidelines in this Internet Use Policy and will adhere to them.

18.7.8 DEFINITIONS

Defamation & libel

What is defamation & libel?

A published (spoken or written) statement or series or statements that affects the reputation of a person (a person can be a human being or an organisation) and exposes them to hatred, contempt, ridicule, being shunned or avoided, discredited in their trade, business, office or profession, or pecuniary loss. If the statement is not true then it is considered slanderous or libellous and the person towards whom it is made has redress in law.

What you must not do

Make statements about people or organisations on any web pages you are including on the website without verifying their basis in fact.

What are the consequences of not following this policy?

You and the Organisation may be subject to expensive legal action.

Harassment

What is harassment?

Words, conduct or action, usually repeated or persistent that, being directed at a specific person, annoys, alarms, or causes substantial emotional distress in that person and serves no purpose.

What you must not do…

Use the internet to harass other members of staff by displaying particular web sites that they consider offensive or threatening.

What are the consequences of not following this policy?

The Organisation deals with harassment by providing advice, support and mediation. Those perpetrating harassment can also be made subject to the Organisation's Disciplinary procedure. *Any proven case of harassment will result in disciplinary action against the guilty party which could ultimately lead to their dismissal.*

Pornography

What is pornography?

Pornography can take many forms. For example, textual descriptions, still and moving images, cartoons and sound files. Some pornography is illegal in the UK and some is legal. Pornography that is legal in the UK may be considered illegal elsewhere. Because of the global nature of Internet these issues must be taken into consideration. Therefore, the Organisation defines pornography as the description or depiction of sexual acts or naked people that are designed to be sexually exciting. The Organisation will not tolerate its facilities being used for this type of material and considers such behaviour to constitute a serious disciplinary offence.

What you must not do

- Create, download or transmit (other than for properly authorised and lawful research) pornography.
- Send or forward web mails with attachments containing pornography. If you receive a web mail with an attachment containing pornography you should report it to the (IM&T) Security officer or your supervisor.

What are the consequences of not following this policy?

- Users and/or the Organisation can be prosecuted or held liable for transmitting or downloading pornographic material, in the UK and elsewhere.
- The reputation of the Organisation will be seriously questioned if its systems have been used to access or transmit pornographic material and this becomes publicly known.
- Users found to be in possession of pornographic material, or to have transmitted pornographic material, may be subject to Organisation disciplinary action.

Copyright

What is copyright?

Copyright is a term used to describe the rights under law that people have to protect original work they have created. The original work can be a computer program, document, graphic, film or sound recording, for example. Copyright protects the work to ensure no one else can copy, alter or use the work without the express permission of the owner. Copyright is sometimes indicated in a piece of work by this symbol ©. However, it does not have to be displayed under British law. So a lack of the symbol does not indicate a lack of copyright. In the case of computer software, users purchase a licence to use the work. The Organisation purchases licences on behalf of its users.

What you must not do

- Alter any software programs, graphics etc without the express permission of the owner.
- Claim someone else's work is your own
- Send copyrighted material by Internet without the permission of the owner. This is considered copying.

What are the consequences of not following this policy?

- A user and/or the Organisation can face fines and/or up to two years imprisonment for infringing copyright.

18.8 Remote Access

18.8.1 Introduction

Remote Access refers to any technology that enables you to connect users in geographically dispersed locations. This access is typically over some kind of dial-up connection, although it can include Wide Area Network (WAN) connections.

18.8.2 Purpose of Policy

Remote access by staff and other no organisations is a method of accessing files and systems that is becoming more common in the business environment. Often, critical business processes such as PACS (Picture Archiving and Communications Systems) rely on easy and reliable access to information systems. In practice, the benefits of securing remote access are considerable – business can be conducted remotely with confidence and sensitive corporate information remains confidential. This document sets out the policy for remote access and includes a set of common controls, which can be applied to reduce the risks associated with a remote access service.

Willful or negligent disregard of this policy will be investigated and may be treated as a disciplinary offence.

18.8.3 Scope

This policy covers all types of remote access, whether fixed or 'roving' including:

- Traveling users (e.g. Staff working across sites or are temporarily based at other locations)
- Home workers (e.g. Clinicians)
- Non clinic staff (e.g. Contractors and other 3rd party organisations)

18.8.4 Objectives

The objectives of the clinic policy on remote access by staff are:

- To provide secure and resilient remote access to the clinic information systems.
- To preserve the integrity, availability and confidentiality of the clinic information and information systems.
- To manage the risk of serious financial loss, loss of client confidence or other serious business impact which may result from a failure in security.
- To comply with all relevant regulatory and legislative requirements (including data protection laws) and to ensure that the clinic is adequately protected under computer misuse legislation.

18.8.5 Principles

In providing remote access to staff, the following high-level principles will be applied:

- A senior member of the clinic will be appointed to have overall responsibility for each remote access connection to ensure that the clinic policy and standards are applied.
- A formal risk analysis process will be conducted for each application to which remote access is granted to assess risks and identify controls needed to reduce risks to an acceptable level.
- Remote users will be restricted to the minimum services and functions necessary to carry out their role.

18.8.6 Responsibilities

- The Registered Manager is ultimately responsible for ensuring that remote access by staff is managed securely.
- The Registered Manager will maintain policy, standards and procedures for remote access to ensure that risks are identified and appropriate controls implemented to reduce those risks.
- The Registered Manager is responsible for confirming whether remote access to business applications and systems is permitted.
- The Registered Manager is responsible for providing authorisation for all remote access users and the level of access provided.
- The Registered Manager will ensure that user profiles and logical access controls are implemented in accordance with agreed access levels.
- The Registered Manager will provide assistance on implementing controls.
- The Registered Manager responsible for assessing risks and ensuring that controls are being applied effectively.
- All **remote access users** are responsible for complying with this policy and associated standards. They must safeguard corporate equipment and information resources and notify the clinic immediately of any security incidents and breaches.
- Users must return all relevant equipment on termination of the need to use remote access.

18.8.7 Risks

The clinic recognises that by providing staff with remote access to information systems, risks are introduced that may result in serious business impact, for example:

- unavailability of network, systems or target information
- degraded performance of remote connections
- loss or corruption of sensitive data
- breach of confidentiality
- loss of or damage to equipment
- Breach of legislation or non-compliance with regulatory or ethical standards.

18.8.8 Security Architecture

The security architecture is typically integrated into the existing Clinic network and is dependent on the IT services that are offered through the network infrastructure. Typical services include:

- Password authentication, authorisation, and accounting
- Strong authentication
- Security monitoring by intrusion detection systems

18.8.9 Security Technologies

To ensure the most comprehensive level of protection possible, every network should include security components that address the following five aspects of network security.

User Identity

All remote users must be registered and authorised by the Registered Manager. User identity will be confirmed by strong authentication and User ID and password authentication. The Registered Manager is responsible for ensuring a log is kept of all user remote access.

Perimeter Security

The Registered Manager will be responsible for ensuring perimeter security devices are in place and operating properly. Perimeter security solutions control access to critical network applications, data, and services so that only legitimate users and information can pass through the network. Routers and switches handle this access control with access control lists and by dedicated firewall appliances. Remote Access Systems with strong authentication software control remote dial in users to the network. A firewall provides a barrier to traffic crossing a network's "perimeter" and permits only authorised traffic to pass, according to a predefined security policy. Complementary tools, including virus scanners and content filters, also help control network perimeters. Firewalls are generally the first security products that organisations deploy to improve their security postures.

Secure Connectivity

The clinic will protect confidential information from eavesdropping or tampering during transmission.

Security Monitoring

Network vulnerability scanners will be used to identify areas of weakness, and intrusion detection systems to monitor and reactively respond to security events as they occur.

Remote diagnostic services and 3rd parties

- Suppliers of central systems/software expect to have dial up access to such systems on request to investigate/fix faults. The clinic will permit such access subject to it being initiated by the computer system and all activity monitored.

- Each supplier or clinic user requiring remote access will be required to commit to maintaining confidentiality of data and information.

- Each request for dial up access will be authorised by the Registered Manager, who will only make the connection when satisfied of the need. The connection will be physically broken when the fault is fixed/supplier ends his session.

18.8.10 User Responsibilities, Awareness & Training

The clinic will ensure that all users of information systems, applications and the networks are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities. Irresponsible or improper actions may result in disciplinary action(s).

18.8.11 System Change Control

All changes to systems must be recorded on a System Change Control form and authorised by the Registered Manager.

18.8.12 Reporting Security Incidents & Weaknesses

All security weaknesses and incidents must be reported to the Registered Manager.

18.9 Confidentiality and security of person identifiable Information

18.9.1 Introduction

The Clinic and its employees have a binding obligation not to disclose information concerning clients' diagnosis, treatment or personal affairs, nor to disclose information relating to individual members of staff. Any such disclosures other than to staff immediately and properly concerned will be regarded as a serious breach of discipline, which could result in dismissal.

Statutory protection is provided for by the Data Protection Act 1998, which covers both electronic and paper recording systems. Further security is provided for by the mandate of the Caldicott Report. The clinic has appointed a Caldicott Guardian who is responsible for safeguarding the release of patient identifiable data. Any patient identifiable data that may be requested is to be authorised before it may be released. The Caldicott Guardian for Brigstock Skin and Laser is Christian Lyons.

The Data Protection Act 1998 also places a statutory duty on the Trust to ensure measures are in place to protect person identifiable information against unauthorised or unlawful use and against accidental loss or destruction of or damage to personal data.

18.9.2 Responsibility

It is the responsibility of the Registered Manager to ensure all staff are aware of this policy.

This policy applies to anyone who may receive client or staff information whilst engaged in their official capacity on clinic premises. This includes:

- All employees of the Trust
- Volunteers
- Student Placements
- Agency Staff

18.9.3 Scope

This policy applies to person identifiable data held in any format.
Examples are:

- Written e.g. casenotes, personal files.
- Verbal e.g. audio tapes.
- Computer e.g. Patient Administration System, person identifiable information held on P.C.
- Visual e.g. X-Rays, Videos, Photographs.

18.9.4 Disclosure of Information

A request for information relating to a clients or member of staff can be received from a number of sources. There are also some groups who, in certain circumstances have a legal right to access information. However the disclosure of information must be in accordance with the provisions of the Data Protection Act. Anyone therefore receiving a request for information relating to a patient or member of staff must follow the appropriate procedure.

18.9.5 Procedure for Processing a Request For information

In all circumstances

- Requests received by telephone should be carefully validated by establishing the identity of the caller.
- Obtain requests for information in writing wherever possible.
- Requests for information from the Police should be referred to the Registered Manager.
- Requests for information from the Press should be dealt with only by the Registered Manager

Requests for Patient Information

- Requests for the release of patient identifiable information to other health/local authority organisations must be authorised by the Caldicott Guardian before release.
- The Clinician responsible for the patients care should be asked to authorise release of the information.
- Patients consent should be sought and recorded within the patients notes before information is released to relatives.
- Requests for information from the Police should be referred to the Registered Manager.
- Subject Access requests for information made under the Data Protection Act 1998 should be processed in accordance with the Clinic Subject Access to Health Records policy 16.10.

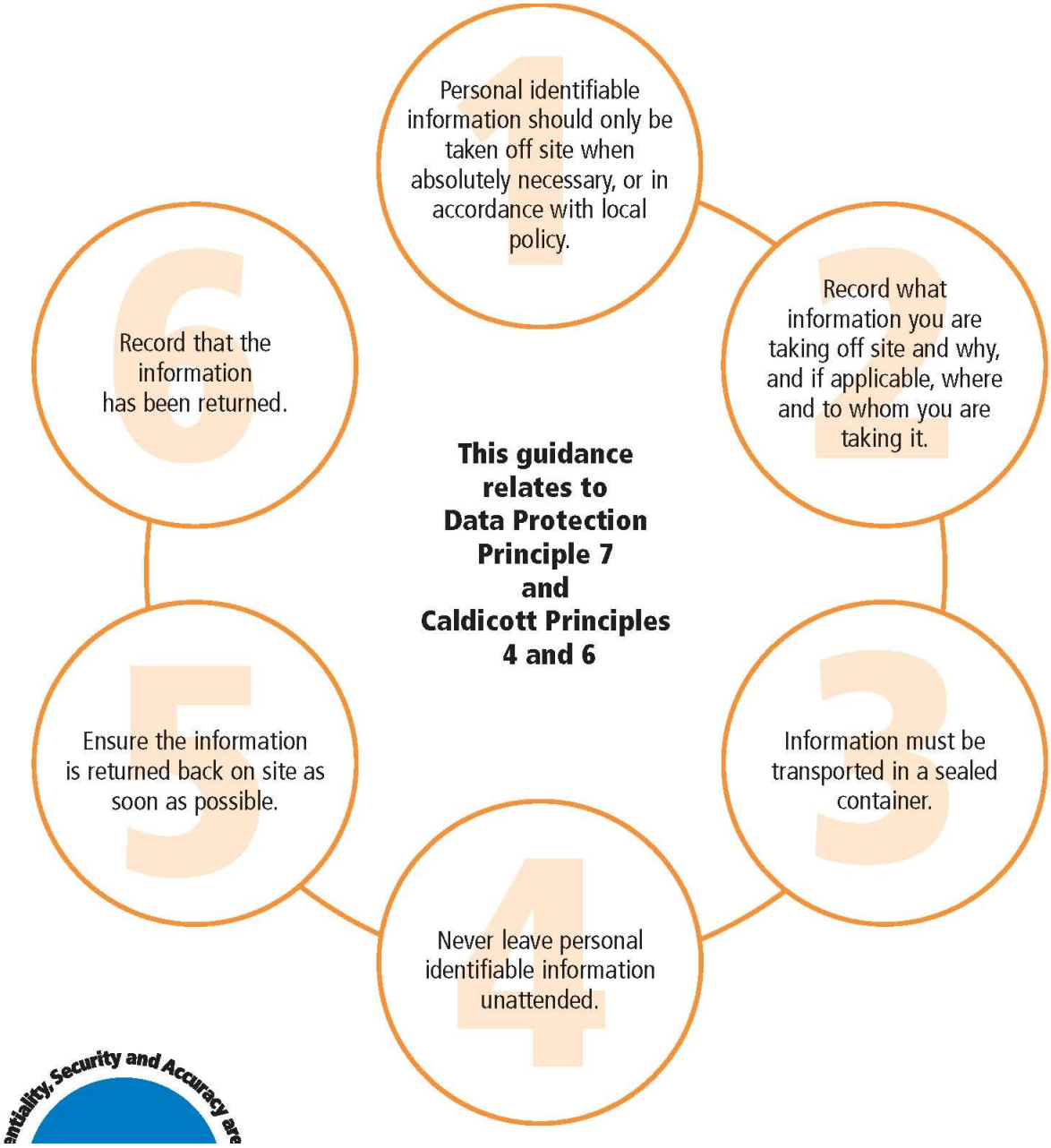
Requests for Information Relating to a Member of Staff

- Requests for information relating to personnel records and financial records should be referred through to the registered manager.

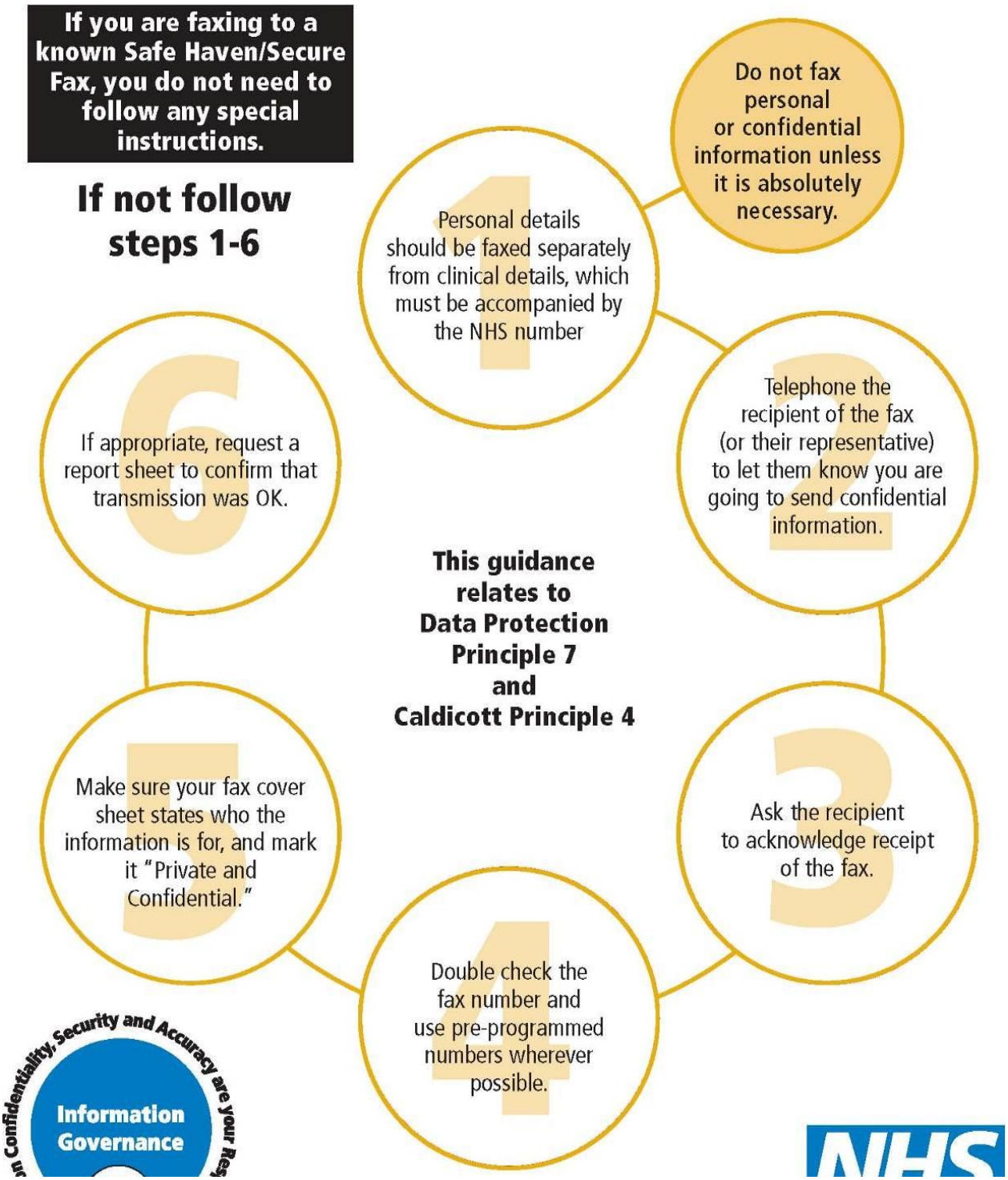
18.9.6 Security of All Person Identifiable Information

- Sight of written or computer based information must be secure against access by unauthorised persons.
- The Registered Manager is responsible for ensuring that Health Records are not accessible to unauthorised persons at any time. When not in use Health Records should be stored in a safe location.
- Access to departments or areas containing confidential information should be restricted to selected personnel only.
- Transportation of confidential information should be entrusted to selected personnel.
- Passwords for use in accessing the data held on computer should restrict access at appropriate levels and provide an audit trail facility.
- Verbal requests for information should be carefully scrutinised and validated.
- Any person removing patient or staff identifiable information (either in electronic or paper based format) from the clinic premises must ensure the following:-
    - The removal of such information is necessary for the purposes of the individuals' job.
    - The information is in a secure location at all times. If held electronically (on floppy disc or CD, for example) files must be password protected.
    - Information should not be left unattended in an employee's vehicle.
    - A record should be made within the department by the person removing it of the information being removed and for what purpose.
    - Confidential electronic information should not be transported on any mobile electronic device without proper password security, which limits access only to authorised user. Mobile electronic devices include (but are not limited to) the following: Handheld PC, PDA, Blackberry, Mobile Telephone, and Lap Top.
    - Electronic mail (e-mail) and other 'messaging' media (e.g. Mobile Telephones) must not be used to transfer patient or staff identifiable information unless it is secured through 'end-to-end' encryption and/or password protection. If any doubts exist on the use of such electronic media transmission the IT department should be contacted to advice.

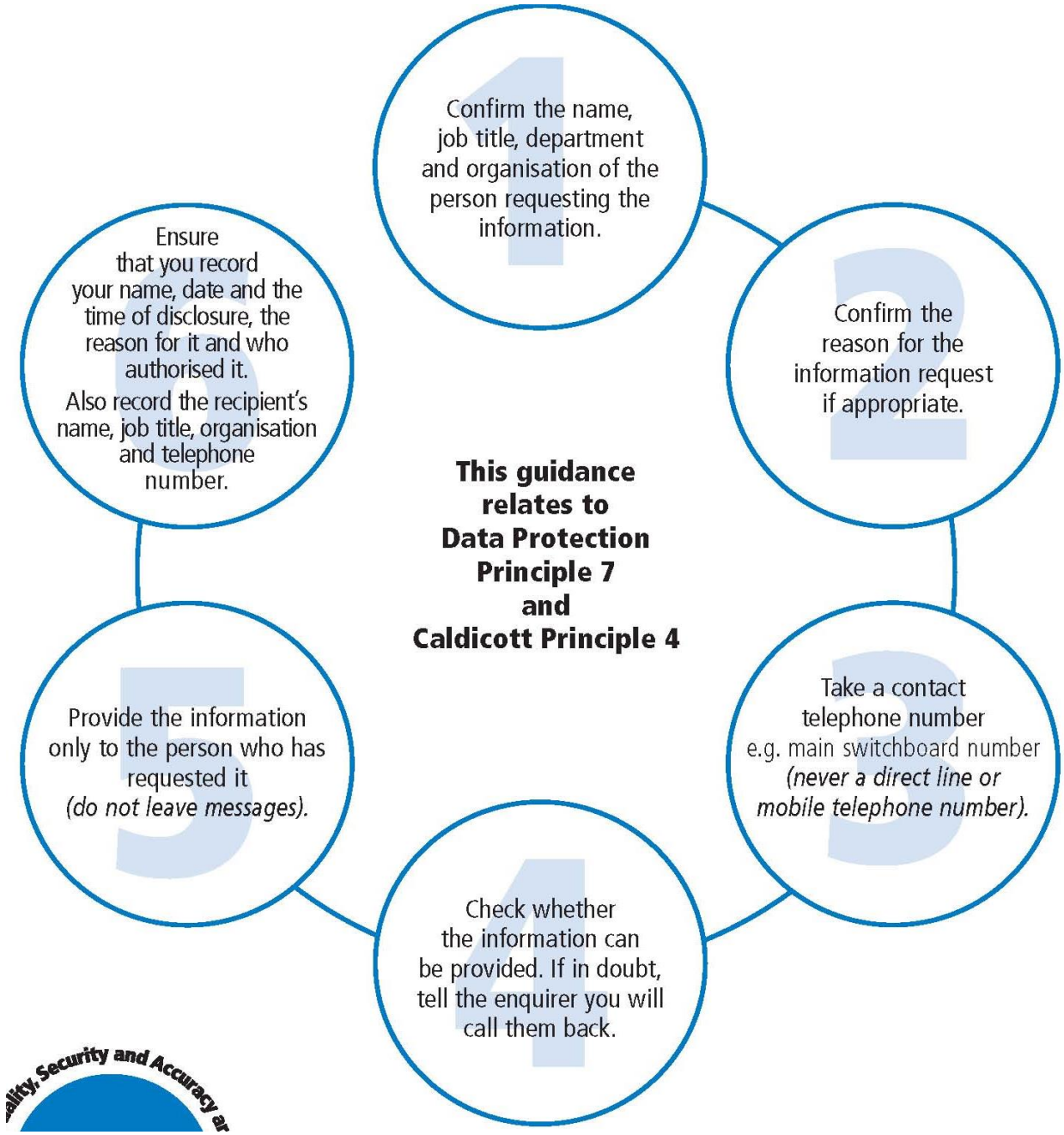
18.9.7 Guidance for the transporting of personal and sensitive information



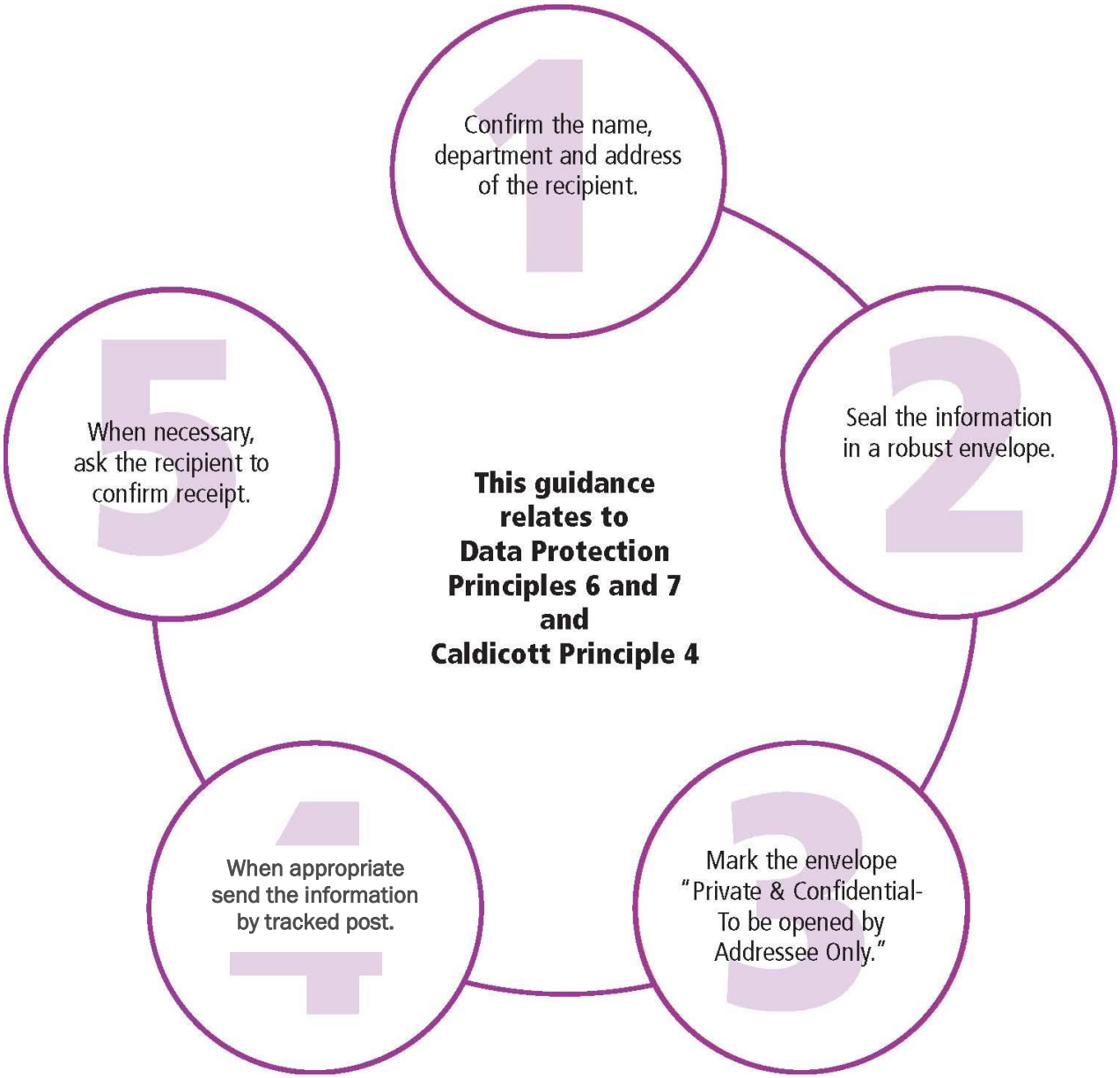
18.9.8 Guidance for sharing personal and sensitive information by fax



18.9.9 Guidance for sharing personal and sensitive information by phone



18.9.10 Guidance for sharing personal and sensitive information by post



18.10 Subject Access to Health Records

18.10.1 Introduction

The clinic and its employees are responsible for ensuring that procedures relating to applications for information in accordance with the Data Protection Act 1998 are adhered to. Access to Health Records is part of this Act.

18.10.2 Scope

This policy applies to all employees of the Clinic.

18.10.3 Responsibility

It is the responsibility of the Registered Manager to ensure all staff is aware of this policy.

18.10.4 Procedure

- Procedure for staff involved in processing applications for information concerning health records is as follows:
- Subject Access requests will be made by the subject.
- On receipt of a request an acknowledgement letter will be sent out to all new requesters.
- Receipt of all applications must be recorded on the Access Data Base.
- Initial applications must be examined carefully to determine their validity.
- All requests for Access to Health Records are to be responded to within the 28 days. 40 days for clients not seen within the past month of request and 21 days for clients seen within a month of request.
- Clinic Clinicians must give authorisation before any case-notes can be released.

18.10.5 Requests for urgent computerised records

If as a matter of urgency a newly registered client medical records are needed.

Requests should be made to the Registered Manager only be made for clients whose records are needed for urgent clinical treatment, not simply needed for administration purposes

18.10.6 Clients Requests

Subjects who notify the clinic of their wish to submit a subject access request are directed to the clinic website where forms can be downloaded or
A copy can be provided by the member of the team dealing with the request. A copy of the form can be found in Appendix 164 - Subject Access Request Form.

Subjects can either be supplied with copies of the case-notes or come into the Clinic and view the original case-notes. If the subject wants to discuss their Medical Information an appointment must be made with the relevant Health Care Professional.

Clients must collect copies of their case-notes from the clinic. The client must bring proof of their identity with them; this must be either a Passport, Photographic Driving License or Photographic ID card. If there is no photographic identification then the client can produce three items of evidence, these can be a utility bill, bank statement and pension or child benefit book or the equivalent documentation showing the requesters address. Patients coming into the clinic to view their notes must show the same proof identification.

The receptionist will check the identity of the subject then take payment where applicable. They will receive a receipt from the receptionist. The copies of case-notes will then be handed to the subject.

18.10.7 Solicitor Requests

All copied notes must be sent by recorded delivery.
The clinic Secretary will be sent a copy of the response form which will have all the details of the charges, enabling the invoice to be issued.

18.10.8 Monitoring

Reports will be produced on a regular basis to ensure the correct procedures within the policy are followed. If any changes are made to the health records act which is part of the data protection act before the policy will be updated at that point, or the policy will be reviewed at the due date.

18.10.9 References

Data Protection Act 1998 (amended 2003)
Access to Health Records Act 1990 (Now part of the Data Protection Act)

18.12 Data Management Policy

18.12.1 Statement

The recording of data within the clinic is under the management and control of the Clinic manager.
. Details of the Clinic Manager can be found here:
N:\nilu christian & reception\Business Continuity Plan\Tel numbers for team - Next of Kin - Key people

The quality of data, the use of templates and the use of specific coding is reviewed on an ongoing basis and the findings are discussed at management meetings, where examples of coding issues are cited as appropriate.

The Registered Manager is responsible for overall coding and data quality issues within the clinic and will ensure accuracy and consistency in coding among both the clinicians and the administrative or casual staff.

The Managing Partner is the non-clinical manager responsible for audit and exception identification and reporting within the clinic.

Any queries should be addressed to the Registered Manager.

18.13 Data Protection Policy

18.13.1 Introduction

The Clinic is a ‘data controller’ and provides a range of services to support clients care.

The Data Protection Act 2018 (DPA) requires a clear direction on policy for security of information held within the clinic and provides individuals with a right of access to a copy of information held about them.

The clinic needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include clients, employees (present, past and prospective), suppliers and other business contacts. The information we hold will include personal, sensitive and corporate information. In addition, we may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or on paper) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 2018.

The lawful and proper treatment of personal information by the clinic is extremely important to the success of our business and in order to maintain the confidence of our service users and employees. We ensure that the clinic treats personal information lawfully and correctly.

This policy provides direction on security against unauthorised access, unlawful processing, and loss or destruction of personal information.

See also: Access to Medical Records policy 2018, which covers Subject Access Requests under the Data Protection Act.

18.13.2 Policy

The general principles underlying the use and sharing of personal information follow the Caldicott principles and data protection principles

- The purpose of using confidential information should be justified
- Only use it when absolutely necessary
- Use the minimum identifiable information for that purpose
- Access should be on a strict need to know basis only
- Everyone must understand their responsibilities to protect information
- Everyone must understand and comply with the law Personal Information

Data protection principles: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

18.13.3 Personal Information

The term ‘personal information’ refers to any information held about an individual who can be identified from that information.

Any information, clinical or non-clinical, held about an identifiable individual must be treated as confidential and must not be made available to anyone who is not entitled to see it.
People have a legal right to choose who has access to their personal information and how it may be used.

Staff should only have access to personal information on a justifiable need to know basis in order for them to perform their duties.

18.13.4 Basic Principles

Any personal information given for one purpose must not be used for another purpose without the consent of the individual concerned because that use may breach confidentiality.
Every member of staff has an obligation to protect confidentiality and a duty to verify the authorisation of another person to ensure information is only passed on to those who have a right to see it.

The rules are there to protect the individual service user and the service provider from breaches of confidentiality, but they should not be applied so rigidly that they are impractical to follow or detrimental to the care of the individual concerned.

All staff should understand their responsibility to protect the confidential information they collect and use and follow the rules and guidance available to them.

If you are unsure about whether or not to disclose information, consult the Data Protection Officer.

18.13.5 Duty of Care

All members of staff must take reasonable care to protect the physical security of confidential information from accidental loss, damage or destruction and from unauthorised or accidental disclosure.
For example:

- Data held on computers, laptops or on disk should be kept physically secure and password protected
- Do not use someone else’s password to gain access to information held on computers
- Always log off when leaving a computer unattended for any length of time

- Medical records should be kept secure and never left unattended in public areas
- Confidential information should only be faxed when there is no alternative and immediate receipt is absolutely necessary for clinical purposes. 'Safe Haven' (1) procedures should be followed
- Envelopes containing patient/client confidential information must be securely sealed, marked 'Private and Confidential' and clearly addressed to a known contact
- Telephone validation procedures (2) must be followed to confirm the identity of telephone callers before information is given to them
- Patient/client information must not be transmitted by email without the use secure end to end servers

If in doubt always seek advice from the Management team

Legislation - Data Protection Act 2018

There are 7 Data Protection principles, which regulate the use of person identifiable data (personal data). The Federation is required to demonstrate compliance with these at all times.

Article 8: Everyone has the right to respect for his private and family life, home and correspondence.

Common Law Duty of Confidence

Information obtained for one purpose should not be used for another purpose without the express or implied authorisation (consent) of the provider of that information.

Freedom of Information Act 2000

The Act gives a general right of access to all types of recorded information held by public authorities, sets out exemptions from that right and places a number of obligations on public authorities.

Data Protection Registration

The clinic is registered with the Information Commissioners Office
Registration Number: ZA323352

Data Protection Officer

The Centre has appointed Nerrisa McLean as the Data Protection Officer. She can be contacted on nerrisamclean@nhs.net

18.13.6 The role of the information Commissioner's Office

The Information Commissioners Office has specific responsibilities for the promotion and enforcement of the Data Protection Act.
Under the Data Protection Act, the Information Commissioner may:

- Serve information notices requiring data controllers to supply him with the information he needs to access compliance.

• Where there has been a breach, serve an enforcement notice (which requires data controllers to take specified steps or to stop taking steps in order to comply with the law).

18.13.7 Clear Desk Policy

At the end of their working day each clinic employee is required to tidy their desk and personal / work related papers into the area provided for that purpose, and remove items into secure storage cupboards if applicable.

In secure administration rooms and offices paperwork should be stored in its designated place. In non-secure administration all paperwork should be cleared into secure areas or locked in cupboards and draws where appropriate.

In any clinical space all paperwork should be cleared to the secure storage provided for each clinician in the admin offices or disposed of as required.

Where keys are used they will be held away from the storage areas.
Everyone who works for the clinic is personally responsible for the tidiness of their working area.

The advantages of this are:

- Confidential information will not be available to casual visitors
- Information storage will be appropriate to the media (e.g. data CDs may go in a fireproof data safe rather than being left on desks
- Information will be held securely whilst not in direct control of the owner
- The workspace will be clear for the next user
- The cleaning team will have clear access to clean working surfaces
- Unnecessary paper will be removed and destroyed regularly

18.14 Data Protection & GDPR Policy For Workers, Employees & Consultants

This policy is designed to be used in conjunction with the Clinic's Records Retention Policy and Computer and Data Security Procedure].

18.14.1 Introduction

The Clinic complies with the legal obligations of the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR'). The Clinic gathers and uses data about workers, employees and consultants, both to manage our relationships with these individuals and in the course of conducting our business.

This Data Protection Policy applies to current and former employees, workers, volunteers, consultants and apprentices ('data subjects').

The Clinic is a 'data controller' for the purposes of these individuals' personal data, and is responsible for determining the purpose and means of the processing of that data.

In line with our Records Retention Policy and Computer and Data Security Procedure, the clinic has measures in place to protect the security of individuals' data. A copy of this can be obtained from the clinic manager.

The clinic will retain data in accordance with our Records Retention Policy. A copy of this can be obtained from the clinic manager. This data will only be held for as long as is necessary for the purposes it has been collected.

This policy has been created to be fully compliant with GDPR and the 2018 Act. Where any conflict arises between those laws and this policy, the Clinic will comply with the 2018 Act and the GDPR.

This policy is separate from data subjects' contracts of employment (or contract for services) and can be amended by the clinic at any time.

18.14.2 The Six Data Protection Principles

The clinic processes personal data in accordance with the six Data Protection Principles for GDPR identified by the ICO, which means it will:

- Be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- Be processed fairly, lawfully and transparently;
- Be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- Be collected and processed only for specified, explicit and legitimate purposes;
- Not be kept for longer than is necessary for the purposes for which it is processed; and
- Be processed securely.

18.14.3 Personal Data

'Personal data' is defined as information relating to a living person ('data subject') that can be used to identify them on its own, **OR** in combination with other information likely to be collected by the Clinic. This applies whether the information is stored physically, electronically, or in any other format.

It **does not** include anonymised data, but **does** include any expression of opinion about the person, or any indication of the intentions of the Clinic or others, in respect to that individual.

Personal data might be provided to the clinic by the individual, or someone else (such as a previous employer or their GP), or it could be created by the clinic. It could be provided or created as part of the recruitment process; in the course of the contract of employment (or services); or after its termination.

The Clinic will collect and use the following types of personal data about staff:

- Contact details and date of birth;
- Recruitment information e.g. application form, CV, references, qualifications etc.;
- Emergency contact details;
- Gender, marital status and family status;
- Information regarding their contract of employment (or services) e.g. start and end dates of employment; working hours; role; location; pension; benefits; holiday entitlement; and salary (including details of previous remuneration);
- Bank details and information in relation to tax status, including National Insurance number;

- Information relating to disciplinary or grievance investigations and proceedings involving them (whether or not they were the main subject of those proceedings);
- Electronic information in relation to their use of IT systems/SMART cards/telephone systems;
- Identification documents e.g. passport; information in relation to immigration status; driving licence; and right to work for the clinic;
- Information relating to an employee's performance and behaviour at work;
- Images (whether captured on CCTV, by photograph or video);
- Training records;
- Any other category of personal data which we may notify you of from time to time.

18.14.4 Special Categories of Personal Data

These comprise personal data consisting of information relating to:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic or biometric data;
- Health;
- Sex life and sexual orientation; and
- Criminal convictions and offences.

The Clinic may hold and use any of these special categories of your personal data in accordance with the law.

18.14.5 Processing Personal Data

'Processing' means any operation which is performed on personal data such as:

- Disclosure by transmission, dissemination or otherwise making available;
- Alignment or combination;
- Collection, recording, organisation, structuring or storage (e.g. within a filing system);
- Adaption or alteration;
- Retrieval, consultation or use; and
- Restriction, destruction or erasure.

The clinic will process individuals' personal data (including special categories of personal data) in accordance with the obligations prescribed under the 2018 Act, including:

- Performing the contract of employment (or services) between the clinic and the individual;
- Complying with any legal obligation; or;
- If it is necessary for the clinics legitimate interests (or for the legitimate interests of someone else). The clinic can only do this in circumstances where the individual's interests and rights do not override those of the clinic (or their own). Individuals have the right to challenge the clinic's legitimate interests and request that this processing be halted.

The clinic may process individuals' personal data for these purposes without your knowledge or consent. The clinic will not use your personal data for an unrelated purpose without informing you about it and the legal basis for processing it.

Please note that if individuals opt not to provide the clinic with some personal data, the clinic may be unable to carry out certain parts of the contract between us, e.g. the clinic needs staff members' bank account details in order to pay them.

18.14.6 When the Clinic Might Process Your Personal Data

The Clinic is required to process individuals' personal data in various situations during their recruitment, employment (or engagement) and even following termination of their employment (or engagement) for reasons including but not limited to:

- Deciding how much to pay staff, and other terms of their contract with the Clinic;
- Ensuring they have the legal right to work for the Clinic;
- Carrying out the contract between the Clinic and the individual including, where relevant, its termination;
- Carrying out a disciplinary or grievance investigation or procedure in relation to them or someone else;
- Monitoring and protecting the security (including network security) of the Clinic, of the individual, other staff, patients and others;
- Paying tax and national insurance;
- Providing a reference upon request from another employer;

- Preventing and detecting fraud or other criminal offences;

The Clinic may process special categories of personal data to use information in relation to your:

- race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and

The Clinic does not take automated decisions about you using your personal data or use profiling in relation to you.

The Clinic will only process special categories of individuals' personal data in certain situations in accordance with the law e.g. with their explicit consent. If the Clinic requests consent to process a special category of an individuals' personal data, the reasons for the request will be explained. Individuals do not need to consent and can withdraw consent later if they choose by contacting the Clinic's Data Protection Officer. Details of the Clinic's Data Protection Officer can be found here:
N:\nilu christian & reception\Business Continuity Plan\Tel numbers for team - Next of Kin - Key people

The Clinic does not need consent to process special categories of individuals' personal data when it is processing it for the following purposes:

- Where it is necessary for carrying out rights and obligations under employment law;
- Where it is necessary to protect individuals' vital interests or those of another person where one or both parties are physically or legally incapable of giving consent;
- Where the individual has made the data public;
- Where processing is necessary for the establishment, exercise or defence of legal claims; and
- Where processing is necessary for the purposes of occupational medicine or for the assessment of the individuals' working capacity.

All employment checks, including those for criminal records, will be carried out in line with current guidance.

18.14.7 Sharing Your Personal Data

Sometimes the Clinic might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

The Clinic *does not* send your personal data outside the European Economic Area. If this changes you will be notified and the protections in place to protect the security of your data will be explained.

18.14.8 Processing Personal Data for the Clinic

All staff who work for, or on behalf of, the clinic has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this Data Protection policy and the Clinic's Records Retention Policy and Computer and Data Security Procedure.

The Clinic's Data Protection Officer is responsible for reviewing this policy and updating the Managing Partners on the Clinic's responsibilities for data protection, and any risks in relation to the processing of data. Any questions related to this policy or data protection should be directed to the Clinic's Data Protection Officer.

All members of staff must follow these rules:

- Staff must only access personal data covered by this policy if needed for purposes necessary to their job, or on behalf of the clinic, and only if they are authorised to do so. The data must only be utilised for the specified lawful purpose for which it was obtained.
- Personal data must be kept secure and not shared with unauthorised people.
- Personal data that is accessed, stored and collected for working purposes must be regularly reviewed and updated. This includes informing the Clinic of changes to your personal contact details.
- Do not make unnecessary copies of personal data. Any unused copies must be kept safe before being securely disposed of.

- Use strong passwords and lock computer screens when not at your workstation.
- Where suitable, anonymise data or use separate keys/codes so that the data subject cannot be identified.
- Do not save personal data to personal computers or other devices.
- Personal data should never be transferred outside the European Economic Area except to comply with the law and with the authorisation of the Data Protection Officer.
- Lock drawers and filing cabinets and do not leave paper with personal data unattended.
- Do not remove personal data from the Clinic's premises without authorisation from your line manager or Data Protection Officer.
- Personal data should be shredded and securely disposed of when it is no longer needed.

Please contact our Data Protection Officer if you have any questions about data protection, or if you become aware of any potential improvements or vulnerabilities in data protection or data security that the Clinic can improve upon.

Any deliberate or negligent breach of this policy may result in disciplinary action being taken in accordance with the Clinic's Disciplinary Procedure.

It is a criminal offence to conceal or destroy personal data which is part of a Subject Access Request. This conduct would be regarded as gross misconduct under the Clinic's Disciplinary Procedure, which could result in dismissal.

18.14.9 Handling Data Breaches

The Clinic has robust measures in place to minimise and prevent data breaches from occurring. Should a breach of personal data occur, the Clinic will make note of the relevant details and circumstances, and keep evidence related to that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then the Clinic will notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact the Registered Manager immediately and retain any related evidence to the breach that you may have.

18.14.10 Subject Access Requests

Data subjects can make a Subject Access Request ('SAR') to access the information the Clinic holds about them. This request must be made in writing. If you receive a SAR you should forward it immediately to the Data Protection Officer, who will prepare a response.

If you wish to make a SAR in relation to your own personal data this should be made in writing to the Clinic Manager. The clinic will respond within one month unless the request is complex or numerous – if this is the case, then the Clinic will need more time to complete the request, and can extend the response period by a further two months.

A Subject Access Request does not incur a fee, however, if the request is deemed to be manifestly unfounded or excessive then Clinic is entitled to charge a reasonable administrative fee, or refuse to respond to the request.

18.14.11 Data Subjects' Rights

In most situations the Clinic will not rely on your consent as a lawful ground to process your data. If the Clinic does request your consent to the processing of your personal data for a specific purpose, you have the right to decline or withdraw your consent at a later time. To withdraw consent, you should contact the clinic manager.

Data subjects have the right to information about what personal data the Clinic processes, how it is processed and on what basis. They have the right to:

- Access their personal data via a Subject Access Request.
- Correct any inaccuracies in their personal data. To do so please contact the Clinic's Data Protection Officer.
- Request that we erase their personal data in the case that the Clinic was not entitled under the law to process it, or the data is no longer needed for the purpose it was collected. In this case, please contact the Clinic's Data Protection Officer.
- Object to data processing where the Clinic is relying on a legitimate interest to do so and the data subject contends that their rights and interests outweigh those of the Clinic and wish us to stop.
- Object if the Clinic processes their personal data for the purposes of direct marketing.
- Receive a copy of their personal data and transfer their personal data to another data controller. The Clinic will not charge for this and will in most cases aim to do this within one month.
- With some exceptions, they have the right not to be exposed or subjected to automated decision-making.

- Be notified of a data security breach (within the appropriate timescales) concerning their personal data.

If you have a complaint about how your data is processed that cannot be resolved with the Clinic, you have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office at www.ico.org.uk.

Where your personal data is being corrected or erased, or the Clinic is contesting the lawfulness of the processing, you can apply for its use to be restricted while the application is made. In this case please contact clinic manager.

18.14.11 Resources

Information Commissioner's Office website
www.ico.org.uk
NHS Employers guidance on criminal checks
www.nhsemployers.org/your-workforce/recruit/employment-checks/criminal-record-check
Records Retention Policy
Computer and Data Security

18.15 PATIENT INFORMATION LEAFLET – GENERAL DATA PROTECTION REGULATIONS

Under the General Data Protection Regulations, from 25th May 2018 clients have the right to apply to see, or have a copy, of their health records. There is **no charge** for these requests except in specific circumstances, such as if the requests are manifestly unfounded, excessive or numerous.

To inform the patients of what GDPR means, we have prepared these information leaflets to help patients to understand;

- What is GDPR
- What 'patient data' means
- What 'consent' means and why they will be asked for it.

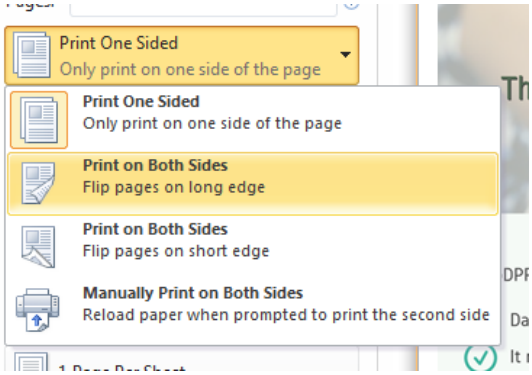
There are two version of the leaflet;

- **Version A** – A4 leaflet (front & back)
- **Version B** – A5 leaflet (front & back)

An electronic version of these leaflets is available on the clinic's website.

If require these leaflets can also be printed double-sided – for any version of MS Word after Windows 2003, you can use the following steps;

- Go to 'File' and choose 'Print'
- Choose the 'Print on both sides' option;



The leaflets have been created to help patients understand the new guidance, and as they are Word documents, they are adaptable and you can amend or add any further information , such as the 'Contact Us' details.

Further Information : QR Code

Patients can scan the QR code with their mobile phone app to find more information from the FPM website

Patient Leaflet – double-click the icon to open

Version A – A4 Leaflet	Version B – A5 Leaflet
Error! Objects cannot be created from editing field codes.	**Error! Objects cannot be created from editing field codes.**

18.16 Records Retention Policy

Record	Retention period (years)	Comments
Accident reports	10	Where litigation has been commenced, keep as advised by legal representatives.
Accounts - Annual (Final - one set only)	Permanent	CQC required period is 30 years
Accounts Minor records (pass books; paying-in slips; cheques counterfoils; cancelled/discharged cheques; accounts of petty cash expenditure; travelling and subsistence accounts; minor vouchers; duplicate receipt books and income records.	6	
Bills, receipts and cleared cheques	6	
Buildings and engineering works, Inclusive of major projects abandoned or deferred - town and country planning matters and all formal contract documents (e.g. Executed agreements, conditions of contract, specifications, "as built" record drawings and documents on the appointment and conditions of engagement of private buildings and engineering consultants.		The general principle to be followed in regard to these records is that they should be preserved for the life of the buildings and installations to which they refer.
Building records (mortgage, transfers, disposal etc)	Permanent	
Buildings and Premises – general maintenance records	3 years	

Cash Books	6	The Limitation Act, 1980
CCTV Images	31 days	Unless retention otherwise justified
Clinical Audit records	5	
Clinical System patient records	Permanent	Retain indefinitely for the foreseeable future
Complaints	10	Where litigations has been commenced, keep as advised by legal representatives
Computerised records	The recommended minimum retention periods apply to both paper and computerised records, though extra care needs to be taken to prevent corruption or deterioration of the data. Re-recording / migration of data will also need to be considered as equipment and software become obsolete. For guidance, see the Public Record Office guidance, Management and Appraisal of Electronic Records (1998) – see link below	
Contracts	6	The Limitation Act, 1980
Death Certificates and death Records	2	
Diaries (office)	1	

Employment Records – see Personnel files and Payroll records below		
Equipment maintenance records	3	
Electrical Testing records	3	
Fire safety Records	5	
Freedom of Information Act Requests	3	
Fridge Temperature Records	1	
Funding data	6	
Insurance certificates	40	
Job advertisements	1	
Job applications and descriptions (following termination of employment)	3	
Medical gas storage, transport and safety	3	
Minutes of Meetings	1	
Out of Hours Records	3	Where these are held as part of the clinical system the longer period of retention relating to clinical system records applies.
Paper Patient Records	20	20 years after last recording. 10 years after death. For patients treated under the Mental Health Act retain for 30 years after last recording.
Payroll / PAYE records	10	For superannuation purposes authorities may wish to retain such records until the subject reaches benefit age. Retain for 10 years after termination of employment

Personnel files (e.g. Personal files, letters of appointment, contracts references & related correspondence)	6	For current staff: See list in **Appendix B** For former staff, keep for 6 years after subject of file leaves service, or until subject's 70th birthday, whichever is the later. Only the summary needs to be kept to age 70; remainder of file can be destroyed 6 years after subject leaves service.
Policies and Procedures (general operating policies)	3 years	Current version and all previous versions to be retained for a minimum 3 year period. 5 years recommended
Purchasing orders excluding medical devices and medical equipment	18 months	
Purchasing orders - medical devices and medical equipment	11 years	
Risk assessments	3	Retain three years and ensure that subsequent risk assessments are available
Rotas and staff duty rosters	4	4 complete years following the year to which they relate
Significant Event records	3	Including those to be notified to the CQC
Superannuation Forms (SD55)	10	
VAT Records	6	Complete years following the end of a VAT period
Water Safety records	5	

The Medical Protection Society recommend that any records not specifically mentioned elsewhere should be retained for 10 years after conclusion of treatment, the patient's death or after the patient has permanently left the country.

Government guidance on employee data: https://www.gov.uk/data-protection-your-business

PATIENT INFORMATION

DATA PROTECTION ACT – PATIENT INFORMATION

We need to hold personal information about you on our computer system and in paper records to help us to look after your health needs, and your doctor is responsible for their accuracy and safe-keeping. Please help to keep your record up to date by informing us of any changes to your circumstances.

Clinicians and staff in the clinic have access to your medical records to enable them to do their jobs. From time to time information may be shared with others involved in your care if it is necessary. Anyone with access to your record is properly trained in confidentiality issues and is governed by both a legal and contractual duty to keep your details private.

All information about you is held securely and appropriate safeguards are in place to prevent accidental loss.

In some circumstances we may be required by law to release your details to statutory or other official bodies, for example if a court order is presented, or in the case of public health issues. In other circumstances you may be required to give written consent before information is released – such as for medical reports for insurance, solicitors etc.

To ensure your privacy, we will not disclose information over the telephone or fax unless we are sure that we are talking to you. Information will not be disclosed to family, friends, or spouses unless we have prior written consent, and we do not leave messages with others.

You have a right to see your records if you wish. Please ask at reception if you would like further details and our patient information leaflet. An appointment will be required. In some circumstances a fee may be payable.

18.17 Computer and Data Security Procedure (Inc. Request to work from home)

18.17.1 Introduction

The purpose of this procedure is to define the arrangements and responsibilities for the physical security of computer hardware, backup of computer data, verification that the backups are effective, and storage of backup data. It also sets out the basis on which software additions may be made to individual PCs, the system or the network.

It is essential that the clinic has full and accessible data backups to ensure that data can be restored in the event of any system failure, meaning normal operations can be resumed quickly and effectively.

There are also a number of precautions to be taken to protect the physical security of computers. These precautions depend on the situation. Different precautions need to be taken for computers used away from the workplace and for laptops used in a variety of locations.

In view of the accidental releases of personal data from a variety of Government organisations it is generally recognised that the risk involved in transporting data “off site” is far greater than the risk of accidental destruction or loss whilst the information is on the premises:

- Patient identifiable information is secure
- Data transfer methods are secure
- That remedial action is being taken if these two issues are weak

In addition:

- Personal identifiable information is not to be stored on removable devices such as CDs, memory-sticks and external hard-drives etc. unless it is encrypted
- Data is not to be downloaded or stored on portable media such as laptops, mobile phones, PDAs etc. unless it is encrypted
- Personal identifiable information is not to be stored on PC equipment in non-secure areas unless it is encrypted.

These requirements apply to all public sector organisations.

Given the complexity of adequate encryption tools, the above requirements will be enforced within the Clinic pending further instructions.

18.17.2 Storage and Backup

Any data stored on a computer hard drive is vulnerable to the following:

Loss due to a computer virus.

Physical loss or damage of the computer, for example:

- Theft
- Water damage
- Fire or physical destruction
- Faulty components
- Software

In particular, there is a risk of breach of confidentiality where a computer is stolen or otherwise falls into unauthorised hands.

The following precautions should be taken:

- Servers should not be used as regular workstations for any application
- Access to servers will be authorised and all server access will be recorded in a dedicated logbook – a locked security system will be used to protect the server
- Use a shared drive on a networked server for all data wherever possible
- No clients data will be stored on a PC or other equipment in non-secure areas
- Use a reputable backup validation service at regular, pre-programmed intervals
- Take extra precautions to protect the server. Servers should be sited away from risk of accidental knocking, spillage of drinks, leaking pipes, overheating due to radiators and be inaccessible to the public
- Where a PC is standalone, ensure that the hard drive is backed up regularly and any confidential data is password protected.

18.17.3 BULK DATA EXTRACTIONS

No bulk extracts or manipulation of data or coding is permitted other than with the prior permission of the Clinic's Data Protection Officer

18.17.5 Protection against Viruses

Data is vulnerable to loss or corruption caused by viruses. Viruses may be introduced from CDROM/DVDROM, other storage media and by direct links via e-mail and web browsing.

The following precautions will be taken:

- Virus protection software will be installed on ALL computer equipment
- There will be a documented procedure for anti-virus software version control and update
- Automatic or pre-programmed updates will be used wherever possible
- A clear procedure via nominated staff will deal with any viruses found

- Software installation will be in accordance with this protocol and only authorised licensed software is to be installed on the organisation's equipment
- The Computer, Internet and Email Policy will contain specific instructions on downloads, attachments and unknown senders etc.
- Ensure that preview panes in email software are not open when sending/receiving mail
- Physical restrictions e.g. drive locks / disable drives will be used where appropriate
- All staff will be made aware of data security issues in all IT-related protocols and procedures
- Data security will be mentioned in the clinic's disciplinary policy

18.17.6 Installation of Software

Software purchases will be authorised by the Registered Manager who will supervise the loading of the software onto the system or individual PCs in accordance with the software licence.

Staff are prohibited from installing or upgrading personal or purchased software without the written permission of the nominated person.

Staff are prohibited from downloading software, upgrades or add-ins from the internet without the written permission of the nominated person.

Staff are permitted to receive and open files received in the normal course of business providing they have been received and virus scanned through the standard virus software installed by the clinical system supplier.

18.17.7 HARDWARE

Staff and contractors are not permitted to introduce or otherwise use any hardware or removable storage devices in the clinic, other than that which has been provided, or pre-approved, by the clinic.

The clinic Manager is responsible for ensuring that the clinic has adequate supplies of removable storage media of a type approved for use in the clinic. The use of removable storage media is by authorised staff only.

Removable storage media (including CDs and other similar temporary items) which are no longer required must be stored securely for destruction along with other PC equipment. The Clinic manager will be responsible for the secure storage of these items.

18.17.8 Protection against Physical Hazards

Water

- Check that the PC or server are not at risk of pipes and radiators which, if damaged, could allow water onto the equipment

- Do not place PCs near to taps/ sinks
- Do not place PCs close to windows subject to condensation and water collection on windowsills
- Ensure that the PC is not kept in a damp or steamy environment

Fire and Heat

- Computers generate quite a bit of heat and should be used in a well-ventilated environment. Overheating can cause malfunction, as well as creating a fire hazard
- Try to place the PC away from direct sunlight and as far as possible from radiators or other sources of heat.
- Normal health and safety protection of the building against fire, such as smoke alarms and CO_2 fire extinguishers should be sufficient for computers. If backup tapes are kept on the premises they must be protected against fire in a fireproof safe
- Have the wiring and plugs checked annually
- Ensure that ventilators on computers are kept clear
- Do not stack paper on or near computers

Environmental Hazards

- Computers are vulnerable to malfunction due to poor air quality, dust, smoke, humidity and grease. A normal working environment should not affect safe running of the computer, but if any of the above are present consider having an air filter. Ensure that the environment is generally clean and free from dust.

Power Supply

- Protect against power surges by having an uninterrupted power supply fitted to the server.

In the event of the premises becoming unusable, a pre-tested 'IT disaster recovery procedure' needs to ensure that systems can be run off site, including replacement hardware.

18.17.9 Protection against Theft or Vandalism via Access to the Building

In addition, the following precautions should be considered to protect the building, such as:

- Burglar alarm with intruder monitor in each room
- Locks on all downstairs windows
- Appropriate locks or keypad access only, on all doors
- Seal off separate areas of the building e.g. reception area should have shutters and a lockable door and all separate rooms should be locked when the building is unoccupied
- Where the building is not fully occupied e.g. during out of hours clinics, only the required rooms and corridors should be accessible to the

public e.g. administration areas and consulting rooms not in use to be kept locked
- Ensure there is a clear responsibility for locking the doors and securing the building when unoccupied
- Ensure any keys stored on site are not in an obvious place and any instructions regarding key locations or keypad codes are not easily accessible
- Have a procedure for dealing with unauthorised access during opening hours
- Ensure keypad codes and alarm codes are changed regularly (monthly) especially after staff leave employment
- Ensure that there is appropriate insurance cover where applicable
- Use bolt-down security server cages
- Do not store patient identifiable information on PC equipment which is not contained in a secure area
- Maintain a separate record of hardware and software specifications of every PC in the building

Specific precautions relating to IT hardware are:

- Use security locks to fix IT hardware to desks to prevent easy removal
- Locate PCs as far away from windows as possible
- Clearly 'security mark' all PCs and all parts of PCs i.e. screen, monitor, keypad.
- Have an asset register for all computer equipment, which includes serial numbers
- Ensure every PC is password protected

18.17.10 Mobile Computing

Particular precautions need to be taken with portable devices, both when they are used on site and when taken offsite.

On-site

Laptops, palmtops and any other portable devices are more vulnerable than PCs, because they are easier to pick up and remove and therefore more desirable to the opportunist thief. It is also less likely, in some circumstances, that their loss will be noticed immediately. However, because of their size, it is possible to provide extra protection:

- When the device is not in use, it should be stored in a secure location
- Where it is left on the premises overnight, it should be stored in a locked cupboard or drawer
- Where the device is shared, have a mechanism for recording who is responsible for it at any particular time
- Patient or personal identifiable information should not be contained on laptops or other portable devices or removable storage devices
- Password protection

In transit

Computers should not be left unattended in cars. Where this is unavoidable, ensures that the car is locked and the computer is out of site in the boot or at least covered up if there is not a boot.

The responsible staff member should take the device with them if leaving the vehicle for any length of time.

Use in a public place
The device should remain with the member of staff at all times

- Care should be taken when using the device that confidential data cannot be overlooked by members of the public e.g. on public transport

Use in a patient's home

- The device should have a password protected screen saver
- The device should remain with the member of staff at all times
- Care should be taken that confidential data cannot be seen by other members of the family / carers

Use on other premises (e.g. outreach clinic)

- The device should remain with the member of staff at all times
- When the device is not in use it should be stored in a secure location
- Where it is left on the premises overnight, it should be stored in a locked cupboard or drawer

18.17.12 Home Working

OVERVIEW

In some instances it may be appropriate for a member of staff to work at home. Careful consideration needs to be given to the following issues:

Will the member of staff have dial-in access to the Clinic's systems?
Will the member of staff be using the confidential data for work purposes or for the individual's own purposes (coursework, research etc)?
Does the staff member require separate registration under the Data Protection Act?

Under no circumstances will patient or personal identifiable information be permitted to be removed from the premises in any format without the express permission of the data controller. Work at home is anticipated to relate to administration or non-personal information only.

Home Workers will be made fully aware of their Information Governance responsibilities. Appropriate forms must be completed to ensure that users understand the terms and conditions for the use of the media in question.

Assurances will also be sought when taking confidential information away from the clinic in paper format. Home workers must ensure that such information will be kept secure and inaccessible to other family members or visitors to the household.

A log sheet will be used to identify individual items being taken out and being returned to the clinic.

For employee's own PC without dial-in access. The following should be considered:

- Consider the physical security of the PC – vulnerability to theft or unauthorised access. Computer equipment should never be left unattended when logged in and switched on. Computer equipment must be kept in a secure place when not in use
- Care should be taken that confidential data cannot be overseen or accessed by unauthorised third parties including other members of the family / visitors to the employee's home
- Risk of loss of the data due to viruses, accidental loss etc. Ensure that up-to-date virus protection is in place and updated regularly
- The device should have a password-protected screen saver
- Back-up of essential data
- Disposal of printouts of confidential data generated at the employee's home
- Ensuring the data is fully deleted from the computer after use
- Ensuring the employee does not use the data for any purpose other than for that authorised
- If the work is ongoing, ensuring that the data is destroyed when the employee leaves employment or replaces their home computer
- If data is backed up using disks or USB sticks these must be password protected and stored in a secure place – any such data backup copies are to be transported securely

Employee's own PC with dial- in access, the following should be considered:

- Remote access to clinic systems should be previously authorised by the Clinic Manager
- Other family members or visitors to the employee's home who use the computer must never have access to confidential data
- The device should have a password-protected screen saver
- Consider the physical security of the PC – vulnerability to theft or unauthorised access. Computer equipment should never be left unattended when logged in and switched on. Computer equipment must be kept in a secure place when not in use
- Ensure that up-to-date virus protection is in place and updated regularly

- Care should be taken that confidential data cannot be overseen by unauthorised third parties including other members of the family / visitors to the employee's home
- Ensure that strong authentication is in place
- Ensure that data is not held on the computer hard drive
- If data is to be backed up using disks or USB sticks, these must be password protected and stored in a secure place – any such data backup copies are to be transported securely
- Ensure that other modems are not attached to the computer, as this invalidates the organisations "code of connection" and places the system's security at risk
- Emailing confidential data to or from a remote PC should only be undertaken when adequate protection is in place
- Ensure proper disposal of printouts of confidential data generated at the employee's home

Using an Organisation's Computer

- Remote access to clinic systems should be previously authorised by the Clinic Manager
- Other family members or visitors to the employee's home who use the computer must never have access to confidential data
- The device should have a password-protected screen saver
- Consider the physical security of the PC – vulnerability to theft or unauthorised access. Computer equipment should never be left unattended when logged in and switched on. Computer equipment must be kept in a secure place when not in use
- Ensure that up-to-date virus protection is in place and updated regularly
- Care should be taken that confidential data cannot be overseen by unauthorised third parties including other members of the family / visitors to the employee's home
- Ensure that other modems are not attached to the computer, as this invalidates the organisation's "code of connection" and places the system at risk
- Ensure proper disposal of printouts of confidential data generated at the employee's home
- Ensure the employee does not use the data for any purpose other than that authorised
- Ensure that no data is held on the computer hard drive where the employee has dial-in access

The Clinic's Responsibilities:

The clinic must ensure that the employee fully understands all their responsibilities with regard to confidential data. The employee must sign a written statement of the responsibilities they are undertaking towards the security of the data.

The clinic must ensure that there are arrangements to clear employees' hard drives of any confidential data as soon as this becomes appropriate.

The clinic must ensure that arrangements are in place for the confidential disposal of any paper waste generated at the employees' home.

The must maintain an up-to-date record of any data being processed / accessed at an employee's home and the purpose for which the employee is accessing the data. It is the employee's responsibility to use the data for the purpose intended and must be absolutely clear as to what that purpose is.

The clinic must be clear as to when it is passing ownership of data to an individual (e.g. for project work or, research and development) and this should be authorised by the Caldicott Guardian / Data Controller. The individual may then need to be separately registered under the Data Protection Act 1998.

RESOURCES

Mobile Phone Policy

Employees who wish to apply to work from home should complete the form Request for authorisation to work from home – shown below:

Request for authorisation to work from home

This form should be completed and submitted to (clinic manager/Caldicott Guardian)

Name _____

Position _____

Clinic _____

Describe the data you intend to work on at home. Indicate the patient identifiers you will hold and any sensitive information such as clinical details.

Explain why the work needs to be carried out away from the workplace.

Please indicate whether you will be working on your own computer or one provided by your employer.

What arrangements have been made to dispose of any paper printouts generated which hold person identifiable data.

I have read, understood and accept the terms of the clinic's computer and data security procedure.

Signed: **Date:**
(employee)

Authorised by:

Signed: **Date:**
(manager)

Print Name: **Position:**

18.18 GDPR – Subject Access Request

18.18.1 Purpose of the Procedure

This document provides guidance on how to process requests under GDPR. It gives a step-by-step sequence of what is required to be done to meet the different types of requests that data subjects can make.

This allows the clinic to gain a better picture of the accuracy and consistency of the process.

18.18.2 Background

General Data Protection Regulation lays down rules about the protection of natural persons in regard to the processing of personal data and the movement of personal data. This regulation protects the fundamental rights and freedom of natural persons and their rights to personal data security.

1. The right of access – providing copies of the information held about an individual
2. The right to rectification – correcting incorrect information
3. The right to erasure – deleting all or partial information about an individual; where consent has been withdrawn and there is no other legal grounds for the processing
4. The right to restrict processing – stopping further processing of an individual data; where consent has been withdrawn, no legal ground for further processing
5. The right to data portability – proving information in a machine-readable format and able to transmit such data to third party upon an individual request
6. The right to object – stopping the processing of an individual data for direct marketing, profiling and where there are no compelling legitimate grounds
7. Rights in relation to automated decision making and profiling - not to be subjected to a decision based solely on automated processing, including profiling of an individual.

18.18.3 Who should use this procedure

This procedure should be used by all members of staff who have the authority to process Data Subject request. The clinic Manager will be the first point of contact and will conduct relevant searches for information

The Procedure

1. The Clinic Manager – This is the point at which requests are received or redirected if by a different member of the team,
2. The Clinic manager will acknowledge receipt of the request
3. Confirm the request type i.e. right to rectification or erasure of personal data
4. Confirm the authentication of the ID provided
5. Log the request and create a folder in on the Shared folder
6. Confirm validity of the request and accept or refuse to process (inform Data Subject)
7. Allocate to appropriate person/department/division/centre/institution that holds the information within 3 days of receiving the SAR

8. Respond to any issues raised by staff
9. Review information provided by staff
10. Respond to SAR – The Clinic manager will be responsible for sending correspondence to the data subject, will redact the data as required and transmit those data to another controller/third party where it has been indicated by data subject without delay; within 2 days of receiving final report.

18.18.4 Timescales

This process must be completed a calendar month of receiving the request. For any delay, please communicate to the data subject using the standard letter template through the Info RIGHTS team.

If more time is needed to respond to complex requests, an extension of another two months is permissible, provided this is communicated to the data subject in a timely manner within the first month. Where it has been agreed not to action the request, data subject must be inform of this decision and advice on the right to complain to the supervisory authority ICO and to a judicial remedy.

18.19 Clinic Privacy Notice

18.19.2 Principles

The clinic has a duty to advice clients of the purpose of personal data and the methods by which patient personal data will be processed.

18.19.3 Status

The clinic aims to design and implement policies and procedures that meet the diverse needs of our clients and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the Equality Act 2010. Consideration has been given to the impact this policy might have in regard to the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment.

18.19.4 Training and support

The clinic will provide guidance and support to help those to whom it applies understand their rights and responsibilities under this policy. Additional support will be provided to managers and supervisors to enable them to deal more effectively with matters arising from this policy.

18.19.5 Who it applies to

This document applies to all employees, partners and directors of the clinic. Other individuals performing functions in relation to the clinic, such as agency workers, locums and contractors, are encouraged to use it.

18.19.6 Why and how it applies to them

Everyone should be aware of the clinics privacy notice and be able to advise patients, their relatives and carers what information is collected, how that information may be used and with whom the clinic will share that information.

The first principle of data protection is that personal data must be processed fairly and lawfully. Being transparent and providing accessible information to clients about how their personal data is used is a key element of the Data Protection Act 1998.

18.19.7 Definition of terms

Privacy notice

A statement that discloses some or all of the ways in which the clinic gathers, uses, discloses and manages a patient's data. It fulfils a legal requirement to protect a patient's privacy.

Data Protection Act 1998 (DPA)
The Data Protection Act (DPA) controls how your personal information is used by organisations, businesses or the government.

Information Commissioner's Office (ICO)
The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

General Data Protection Regulation (GDPR)
The GDPR replaces the Data Protection Directive 95/46/EC and was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way in which organisations across the region approach data privacy. The GDPR comes into effect on 25 May 2018.

Data controller
A person who (either alone or jointly with other persons) determines the purposes for which and the manner in which any personal data is, or is to be, processed.

Data subject
An individual who is the subject of personal data.

18.19.8 Compliance with regulations

GDPR
In accordance with the GDPR, this clinic will ensure that information provided to subjects about how their data is processed will be:

- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge

DPA 1998
In accordance with the DPA 1998, this clinic will ensure that any personal data is processed fairly and lawfully and:

- The clinic will not use the data in ways that have unjustified, adverse effects on the individuals concerned;
- We will be transparent about how we intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- We will handle people's personal data only in ways they would reasonably expect; and we will not do anything unlawful with the data

Communicating privacy information
At the clinic, the clinic privacy notice is displayed on our website, through signage in the waiting room, and in writing during patient registration. We will:

- Inform patients how their data will be used and for what purpose
- Allow patients to opt out of sharing their data, should they so wish

What data will be collected?
At The clinic, the following data will be collected:

- Patient details (name, date of birth)
- Address and NOK information
- Medical notes (paper and electronic)
- Details of treatment and care, including medications
- Results of tests (Histopathology reports)
- Any other pertinent information

Privacy notice checklists
The ICO has provided a privacy notice checklist which can be used to support the writing of the clinic privacy notice. The checklist can be found by following this link.

Privacy notice template
A privacy notice template can be found at Appendix 157 with a series of notices for the following detailing specific uses or sharing of personal information including the legal basis for the processing:

- Call Recording
- CQC
- Direct Care
- Emergencies
- Payments

18.19.9 Summary

It is the responsibility of all staff at the clinic to ensure that patients understand what information is held about them and how this information may be used. Furthermore, the clinic must adhere to the DPA 1998 and the GDPR, to ensure compliance with extant legal rules and legislative acts.

18.20 DATA PROTECTION IMPACT ASSESSMENT (DPIA) POLICY

18.20.1 Introduction

This policy reinforces the principles of Information Governance and Data Protection. The document outlines the clinic's approach and methodology for Data Protection Impact Assessments for new and existing systems and processes.

It is important that all new processes, policies, projects, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements.

The policy details the process to be followed to ensure a formal assessment is completed to determine whether any proposed changes to the clinic's processes, policies, projects and/or information assets impacts on the integrity and accessibility of personal information.

Some of the considerations that should be taken into account are whether a new process, project or information asset will:

- Affect the quality of personal information already collected;
- Allow personal information to be checked for relevancy, accuracy and validity;
- Incorporate a procedure to ensure that personal information is disposed of through archiving or destruction when it is no longer required or in accordance with The Records Management: Code of Practice;
- Have an adequate level of technical and organisational security measures to ensure that personal information is protected from unlawful or unauthorised access and from accidental loss, destruction or damage;
- Enable data retrieval to support business continuity in the event of an emergency;
- Enable the timely location and retrieval of personal information to meet a subject access request; and
- Alter the way in which the clinic captures information within / monitors information from a key system.

The rationale for conducting a DPIA is to:

- Identify and manage risk;
- Avoid unnecessary costs and inadequate solutions;
- Avoid loss of trust and reputation;
- Inform the clinic's communications strategy; and
- Meet legal requirements in terms of information security, data protection and confidentiality.

The policy applies to information held in both manual and electronic form.

This policy applies to all staff who works for the clinic including contractors, who are responsible for project managing a new project, implementation of a new process or plan to modify a current system (information asset).

18.20.2 Data Protection Impact Assessment (DPIA) Process

A DPIA must be carried out in addition to compliance checking or a data protection audit, and conducted at a stage when the outcome can genuinely affect the development of a project or process. A Data Protection Impact Assessment Tool can be found here: Appendix 163 - Data Protection Impact Assessment Tool

An effective DPIA will help identify and avoid problems which may not be obvious at the conception stage and should form an intrinsic part of the overall risk assessment.

18.20.3 When should a DPIA be undertaken?

Not every new project, system or change in process will require a DPIA. The Information Commissioner's Office (ICO) recommends that DPIAs are completed to comply with a change in law, introduction of new or intrusive technology or where person identifiable or sensitive information which was originally collected for a limited purpose is going to be collected for any new purpose(s) or reused in a new and unexpected way.

Completion of the initial DPIA Screening Questionnaire (Appendix 1) will ensure that a full DPIA is completed only when necessary and provide evidence to support the Clinics' Information Governance agenda.

Best practice dictates that the initial screening questionnaire should be started when:

- The project / process is being designed and the scope has been agreed;
- Before a system has been procured;
- Before contracts/MOUs/agreements have been signed.

- For all QIPP projects as a mandatory assessment within each Project Initiation Document (PID)

18.20.4 Who Is Required to Complete a DPIA?

The initial screening questionnaire should be completed by the Information Asset Owner (IAO) or delegated to the individual responsible for overseeing the implementation of the project / process / policy / amendment to an existing system (such as the project manager).

18.20.5 Applying the Outcome of the Initial Screening Questionnaire

Where answers to questions are 'Yes', a full scale DPIA should be completed

Definitions

Data Protection Impact Assessment	A risk technique mandated by the General Data Protection Regulations to enable organisations to address privacy concerns and ensure appropriate technical and organisational safeguards are addressed and built in to new projects / processes / policies / amendments of existing systems
Projects / processes / policies / amendments of existing systems	DPIAs are required when new projects occur (e.g. introduction of a new electronic patient record, process involving the transfer and/or use of information between providers of a service) or where plans are proposed to develop an existing information asset. These can be both paper and electronic.
Special Category data	Under the Data Protection Act this is data such as patient diagnosis, medical history, ethnicity, sex, religion.
Personal data	Data which is capable of identifying an individual, but isn't classified as special category data, for example, name, postcode, GP, next of kin, address, date of birth and so on.
Privacy-invasive technology	Privacy-invasive software is a category of computer software that ignores users' privacy and that is distributed with a specific intent, often of a commercial nature/mass marketing, which negatively affects its users. Examples include, but are not limited to, locator technologies such as global positioning systems (GPS) and mobile phone locators, biometric scanners.

18.20.6 Roles and Responsibilities

The Partners

The Partners owns the information governance strategy & framework and the implementation of measures to minimise information risk and safeguard the interests of its staff, clients and information assets of the clinic.

Senior Information Risk Owner (SIRO)

The SIRO is responsible to the Partners for ensuring an Information Governance strategy & framework is implemented, reviewed and its effect monitored. Privacy Impact Assessment is one element of the management of IG and information risk.

The SIRO will:

- Take ownership of the Clinic's information risks;
- Occupy a key role in ensuring effective management and identification of information risks.
- Oversees all QIPP projects and ensure they have a completed PIA

Information Asset Owners

An Information Asset Owner has responsibility for managing aspects of the clinic's business, and therefore will be responsible for knowing what information assets are held by their team, understanding the potential risks to the assets and to provide assurance to the Clinic's SIRO concerning the security, confidentiality, integrity and use of the assets. Their roles include:

- Understanding what information is held;
- Knowing what is to be added and removed;
- Knowing how information is moved / transferred;
- Knowing who has access and why; and
- Ensuring compliance with the relevant legal frameworks, i.e. consent and confidentiality

Information Asset Administrators

As an Information Asset Administrator, with day-to-day responsibility for the creation, receipt, use and storage of information assets, IAAs will provide support to the Information Asset Owner for their team to ensure that:

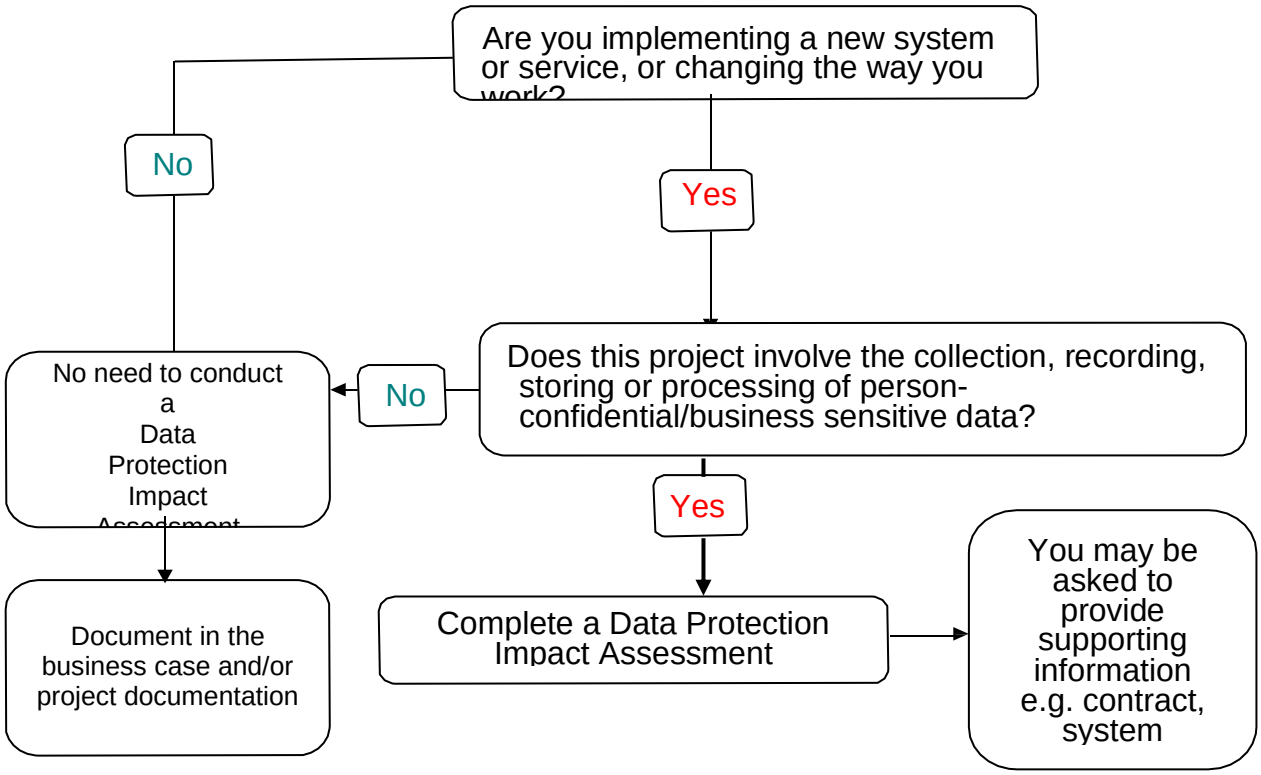
- The Information Asset Register is kept up to date
- Policies and procedures regarding information management and risk are followed

- Actual or potential information risks are recognised and reported; and
- Information sharing agreements are complied with.

Data Protection Office (DPO)

The DPO is responsible for assessing and manage the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing. This will be achieved by reviewing the outcome of the DPIA to ensure compliance with the GDPR and national data protection legislation is maintained.

Appendix 1 - Do I Need to Complete a Data Protection Impact Assessment questionnaire?



When deciding whether a DPIA questionnaire is required, if the first answer is 'yes', but the second response is 'unsure', please complete the questions in section 1 of the DPIA questionnaire to assist the decision.

The questionnaire will be reviewed by the Data Protection Officer, and the recommendation from the questionnaire will be notified to the Project Manager / Information Asset Owner. The recommendation will be either:

1. A full DPIA is required where the new process or change of use of PCD/Business Sensitive data requires more thorough investigation; or

2. The DPIA questionnaire will be signed off by the Data Protection Officer, the PIA log updated by the Data Protection Officer and the outcome reported to the IG team.

18.21 DATA QUALITY POLICY

18.21.1 Introduction

Brigstock Skin and Laser aspires to the highest standards of corporate behaviour and clinical competence, to ensure that safe, fair and equitable procedures are applied to all organisational transactions, including relationships with clients, the public, staff, stakeholders and the use of public resources.

In order to provide clear and consistent guidance, the clinic will develop documents to fulfil all statutory, organisational and best practice requirements and support the principles of equal opportunity for all.

The Clinic recognises that all of their decisions, whether health care, managerial or financial, need to be based on information which is of the highest quality. Data quality is crucial and the availability of complete, accurate, relevant and timely data is important in supporting patient/service user care, governance, management and service agreements for health care planning and accountability.

18.21.2 Purpose and Scope

This policy is designed to ensure that the importance of data quality within the Clinic is disseminated to all staff.

It will describe the meaning of data quality, who is responsible for its maintenance and how it can continue to improve in the future.

Although this policy relates to clients data and information, the principles included are applicable to any other data/information staff may encounter i.e. recording of minutes, etc.

18.21.3 Duties and Responsibilities

3.1 The Registered Manager of the clinic has overall responsibility for data quality

3.2 All system managers (Information Asset Owners) must ensure that procedures are upheld for each personal confidential data system.

3.3 It is the responsibility of the organisation to ensure an audit programme is in place to assess compliance with the policy and to ensure training requirements are identified and actioned for relevant staff.

3.4 It is the responsibility of line managers to ensure staff compliance with local data quality procedures and to ensure that staff complies with good practice in data quality.

3.5 Reference to the responsibility towards data quality will be included in relevant job descriptions and all users must comply with this policy, related policies and relevant legislation and national guidance.

18.21.4 Definitions

Data: Data is a collection of facts from which information is constructed via processing or interpretation.

Information: Information is the result of processing, gathering, manipulating and organising data in a way that adds to the knowledge of the receiver.

Data Quality: Data quality is a measure of the degree of usefulness of data for a specific purpose.

18.21.5 Data Quality

Importance of Data Quality

A vast amount of data is recorded when caring for clients in commissioned services. Having accurate, relevant information that is accessible at the appropriate times is essential to each and every health management or business decision and to the success of the service provided. With this in mind, it is essential that all employees of the clinic recognise the importance of data quality and their responsibilities in this area.

Quality information is essential for:

- The delivery of effective, relevant and timely care, and to minimise risks to clients
- Efficient administrative and health care processes, such as communication with clients and professionals involved in their treatment/care
- Management and strategic planning, requiring accurate information about the volume and type of health care activity to provide appropriate allocation of resources and future service delivery
- Establishing acceptable service agreements for health care provision
- Health care governance, which depends on detailed, accurate patient data for the identification of areas where health care could be improved
- Providing information for other organisations – these organisations depend on the information we send them and need to have confidence in its quality
- Being able to allow local and national benchmarking
- Budget Monitoring, including Payment by Results, and financial planning to support
- service delivery

It is also important to ensure that the data quality is of a high standard in order to comply with the Data Protection Act in particular principle 4, ‘accurate and up-to-date’.

Data Standards

The use of data standards within systems can greatly improve data quality. These can be incorporated into systems either using electronic validation programmes which are conformant with the clinic's standards, e.g. drop down menus, or manually generated lists for services that do not yet have computer facilities. Either method requires the list to be generated from nationally or locally agreed standards and definitions, e.g. for the clinic practice codes, ethnicity, etc. These must be controlled, maintained and updated in accordance with any changes that may occur, and in addition electronic validation programmes must not be switched off or overridden by operational staff.

Where no national standards exist

In certain situations there will be no applicable standards. In these instances, the Clinic will agree local standards as part of the contracting process. It is important that any local standards are subject to annual reviews within the clinic as there will be no automatic input received from national sources. This process will ensure their validity and continued relevance.

Data Validation

Importance of validation

Validation encompasses the processes that are required to ensure that the information being recorded is of good quality. These processes deal with data that is being added continuously and also can be used on historical data to improve its quality.

It is imperative that regular validation processes and data checks/audits are undertaken on data being recorded to assess its completeness, accuracy, relevance, accessibility and timeliness. Such processes may include, checking for duplicate or missing data, validating waiting lists and patient's numbers are used and validated.

Validation methods

Validation should be accomplished by using techniques that are in line with the legal powers of the clinic.

Synchronising information systems

In situations where data is shared or is common between systems it is imperative that the source data be validated initially. Any modifications made to this data must then be replicated in other related systems, ensuring there are no inconsistencies between them. Synchronisation between systems is required to ensure that all data sources reflect the same information.

Timescales for validation

Where inconsistencies in data and information are identified these must be acted upon in a timely fashion and documented. Locally agreed deadlines will apply to the required corrections but all amendments should be made within a maximum of two months from the identification date.

Monitoring of Data Quality

As commissioning organisations, the clinic has the responsibility of monitoring the data quality of the services it commissions. This will be carried out in a variety of ways according to the type of service and the data it collects.
Examples include Patients' number compliance, (where appropriate) pseudonymisation. The responsible team member will report the monitoring of data quality to the responsible committee in accordance with agreed timescales.

Policy Review

This policy will be reviewed annually in line with Information Governance Toolkit requirements or where changes occur with legislation or national policy.

Related Policies

This policy links to a number of other clinic policies and all staff should be aware of these and their responsibilities to the organisation in complying with their content. (Information regarding which policies are relevant should be sought from the clinic Manager). These include:

- Data Protection Policy
- Information Security Assurance Policy
- Records Management Policy

18.22 INFORMATION SECURITY ASSURANCE POLICY

18.22.1 Introduction

This policy shall apply to the information, systems, networks, applications, location and staff at the clinic. The clinic should consider the physical security of its assets, i.e. its premises, equipment and information. Additionally the safety of clinic employees should be taken into account. Meeting the requirement involves putting measures in place to delay and prevent unauthorised access, to detect attempted or actual unauthorised access, and to ensure that there are procedures to be followed in the event that unauthorised access does occur.

18.22.2 Purpose of the policy

To enable and to maintain the effective security and confidentiality of information processed and stored at the clinic.

18.22.3 Securing premises

Rooms should preferably be locked when not in use, even for short periods of time. This is particularly important when sensitive documentation is stored in the room. Windows on ground floor rooms are favourite access points for burglars and, particularly during hot weather, staff should ensure that they are closed when the room is not occupied. The use of window locks is present for all ground floor rooms.

Motion detection alarm systems should be fitted in all ground floor offices and restricted area offices and switched on when the offices are not in use.

Physical keys are issued on a need-to-have basis and electronic access cards to doors are issued in the same way. Both items have to be returned when the user leaves the clinic employment. Personnel are briefed on the importance of reporting lost keys. Identity badges and other equipment are returned when an employee leaves the Clinic. Door keys and fobs are handed back to the Clinic Manager and returned from where they were issued.

18.22.4 Clear desk and clear screen policy

Brigstock Skin and Laser staffs clear their desks of all sensitive and confidential information when they leave the room and ensure that such information is locked securely away overnight. Staffs leave their computers in “logged off” or “locked” state when going for lunch or leaving their computer unattended for a long period of time.

18.22.5 Prevention of unauthorised access

The clinic owns expensive equipment, such as computers, fax machines, phones, photocopiers etc., and they will also hold vital and confidential information in various forms. The information could be written on paper, or photograph, stored on floppy or compact disc, or stored electronically on a computer. Brigstock Skin and Laser’s assets should be protected with appropriate security barriers and entry controls. Additionally the Clinic should ensure that all staff is protected from violence.

Brigstock Skin and Laser Centre have measures to secure the grounds by using large iron gates to prevent access to the car park area after clinic hours. Should access be gained then there are internal locks on all windows and doors as well as a security monitoring system. The details and levels of protection and prevention are outlined in the chart below.

There are many different ways that Brigstock Skin and Laser can protect its property and personnel. These are outlined in the table below.

	Premises	Equipment	Other Assets	Preventative / Action Plans
	• Alarm door fobs. • Magnetic door lock keys. • Keypad access to certain areas of the building. • Building Alarm. • Main Gate locked to car park. • Fire prevention and drills. • Internal Window locks. • Staff “panic” alarms for	• Personal passwords. • Personal logon to computers. • Main Servers are locked. • Company “smartcards”. • Leased or loaned IT equipment is pass coded.	• Patient records secured in vault. • Backup and Data tapes secured in vault. • Fireproof safe for storage tapes (backup) • Controlled Drugs Safe. • Drugs fridges.	• Clinic’s Business Contingency Plan. • Equipment assets register. • Locking up procedure.

	protection.	• Protection from malicious software with anti virus software.		

18.23 RECORDS MANAGEMENT POLICY

18.23.1 Introduction

Records management is vital to the delivery of our services in an orderly, efficient, and accountable manner. Effective records management will help ensure that we have the right information at the right time to make the right decisions. It will provide evidence of what we do and why.

18.23.2 Scope

The Clinic Manager in conjunction Data Protection Officer (DPO) has the overall responsibility for the implementation of this policy in the team with day-to-day responsibility.

A record is information created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations.

Our records can be in either paper or electronic format and both formats are covered by this policy. This document sets out the overall framework within which The BRIGSTOCK SKIN AND LASER CENTRE manages records.

All records created are the property of the Clinic and managed in conjunction with this policy.

18.23.3 Responsibility for Records Management

All members of staff, who create, store, receive and use records must:

- Treat records as a resource and ensure as far as practicably possible that records are accurate and filed in such a way that they can be easily located
- Keep records no longer than they are needed; see retention schedule
- Keep confidential records in a secure environment
- Keep records stored in a safe and cost-effective way
- Allow people to access information only if they need or have a right to do so
- Create records that are accurate and that do not defame another individual, expose BRIGSTOCK SKIN AND LASER to unnecessary risk or to tamper with records in a way that risks them becoming inaccurate
- Save long term records in an open source or archival format to ensure readability even if systems change

Relevant legislation, professional standards and policies

The Clinic Manager will be responsible for BRIGSTOCK SKIN AND LASER CENTRE being compliant with legislation and professional standards which are relevant to the area of records management.

The DPO, Nerrisa Mclean will ensure that BRIGSTOCK SKIN AND LASER CENTRE records management systems and procedures inter-relate with

other internal policies, such as those produced in the areas of archiving, business continuity policy and information security. The identification and maintenance of important records is a vital element of BRIGSTOCK SKIN AND LASER CENTRE business continuity work.

18.23.4 Training

The Clinic Manager in conjunction with the Registered Manager will be responsible for organising an appropriate amount of level of training for relevant members of staff.