1 Introduction

This document sets out Aseptika's approach to managing security, confidentiality, data quality and records.

2 Information Governance Framework

Heading	Notes
Senior Roles	• Senior Information Risk Owner (SIRO) - Managing Director • Caldicott Guardian - Quality Manager • Data Protection Officer - Quality Manager • Accountability for record keeping – Quality Manager
Key Policies	• Information Security Policy • Overarching IG policy • IG staff handbook. • Data Protection Policy • Network Security Policy • Record Retention Schedule All policies and procedures will be subject to regular review.
Key Governance Body	Management Meeting
Governance Framework	Information Governance is discussed at monthly management meetings with a specific agenda set for six monthly management meetings. Attendees of the management meetings: • The MD (SIRO) • Quality Manager (Caldicott Guardian, DPO) • Office Manager • Software Developer Manager • Technical Director • Finance Manager The schedule for covering IG items at the Management Team meeting is set out in Section 4. Information governance requirements are included in staff contracts. Non-disclosure agreements are used where appropriate.
Training & Guidance	An IG staff handbook is in place. The Caldicott Guardian will complete the Role of the Caldicott Guardian Workbook (or e-learning). The SIRO will complete the Introduction to Risk Management for SIROs and IAO's Workbook (or e-learning). All Aseptika staff will undertake e-learning in security and data protection on an annual basis.
Incident Management	See section 13

3 Responsibilities

3.1 The Senior Information Risk Owner (SIRO)

The SIRO takes overall ownership of Aseptika's information risk policy, implements and leads the risk assessment and management processes and review's the effectiveness of the process.

Key Responsibilities

- Oversee the risk management arrangements and assures that Aseptika remains compliant with NHS Data Protection & Security Toolkit policy, Cyber Essential Plus Certification, standards and methods.
- Take ownership of the assessment processes for information risk.
- Ensure that Aseptika is kept up to date and briefed on all information risk issues affecting the organisation and its business partners.
- Review and agree actions in respect of identified information and clinical data risks.
- Ensure that the approach to information risk is appropriately communicated to all staff.
- Provide a focal point for the escalation, resolution and/or discussion of information risk issues.
- Ensure that identified information threats and vulnerabilities are followed up for risk mitigation, and that perceived or actual information incidents are managed in accordance with NHS Data Security & Protection Toolkit requirements as set out by the Commissioner.
- To monitor compliance with the policy throughout the organisation and to develop procedures for effective security.
- To arrange and / or provide information security education and training.
- To develop and monitor a formal procedure for reporting information security incidents and investigations.
- To contribute to the business continuity planning process.
- To advise on the control and monitoring of copying of proprietary software.
- To advise on and monitor the safeguarding of organisational records.
- To ascertain the extent to which information collected, held and/or used in the organisation is properly controlled and safeguarded from loss of confidentiality, integrity or availability from any cause.
- To identify and test the controls and, where appropriate, to suggest additional controls, which may be established to maintain the confidentiality, integrity and availability of information.

3.2 The Caldicott Guardian

A Caldicott Guardian is a senior role responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Caldicott Guardian plays a key role in ensuring that Aseptika staff, along with partner organisations, satisfies the highest practicable standards for handling patient identifiable information. Acting as the 'conscience' of Aseptika, the Caldicott Guardian actively supports work to enable information sharing where it is appropriate to share and advises on options for lawful and ethical processing of information.

The Caldicott Guardian represents and champions confidentiality requirements and issues at management meetings.

In this role the Caldicott Guardian will also be responsible for ensuring that internal audits of data confidentiality are undertaken.

Key Responsibilities

- Ensure that patient consent forms are provided to patients.
- Ensure that patient's requests for access to their own information is processed in a timely manner.
- Ensure that any patient (clinical) information released to external organisations are subject to suitable pseudonymisation prior to being released or as applicable.
- A review of existing flows of patient information.
- A review of database construction and management where any patient information is stored.
- A review of procedures for handling patient-identifiable information generally, including information collected by Aseptika and used in its dealings with other organisations, e.g. during clinical trials or providing services to the NHS.
- Defining escalation and handling procedures for any information breaches, including the need to notify other organisations.
- Development of an improvement plan to address any identified deficiencies.

3.3 Data Protection Officer (DPO)

The DPO will drive compliance with the EU General Data Protection Regulation (GDPR) and ensure ongoing compliance of all core activities for Aseptika.

Key responsibilities

- The Data Protection Officer will maintain expert knowledge of data protection law and practices, as well as other professional qualities, to ensure that Aseptika complies with the requirements of the EU GDPR and relevant data protection law(s) and regulations.
- Reporting directly to Managing Director, the Data Protection Officer must inform and advise on the protection of personal data in relation to the EU GDPR and relevant law(s) and regulations.
- The DPO will ensure that documentation to demonstrate compliance with the GDPR such as policies and procedures are kept up to date. For example, the register of processing required under Article 30.
- Furthermore, the DPO will plan and schedule data processing audits regularly, monitoring core activities to ensure they comply with the EU GDPR.
- The Data Protection Officer is the main contact point for employees and will liaise with all members of staff on matters of data protection.

Key tasks of the Data Protection Officer (Article 39, (1) and Recital 97):

a) To inform and advise all members of staff on their obligation to adhere to the EU GDPR and relevant law(s) when dealing with personal data.
b) To monitor compliance with the EU GDPR and relevant law(s).
c) Advise and inform on the data protection impact assessment (DPIA), including monitoring performance of DPIAs against the requirements of the EU GDPR Article 35.
d) Liaise and cooperate with the supervisory authority.

e) To be the point of contact for the supervisory authority on issues relating to processing of personal data, and to consult with the supervisory authority, where necessary, on any other personal data matters.
f) To contribute to the development and maintenance of all Aseptika's data protection policies, procedures and processes in relation to the protection of personal data.
g) Advise management on the allocation of responsibilities internally to support ongoing compliance with the EU GDPR and UK law(s).
h) Ensure training and awareness is available and delivered to all members of staff involved in processing operations relating to personal data.
i) Regularly monitor compliance with the EU GDPR and relevant data protection law(s) by conducting audits of processes relating to personal data, and report to the MD.
j) To be the point of contact for data subjects about the processing of their personal data.
k) To monitor compliance with the Data Protection Policy and to develop/advise on procedures for effective security.
l) To advise senior management on the allocation of information security responsibilities.
m) To develop/advise on formal procedures for reporting incidents (EU GDPR and information security-related) and investigations under Articles 33 and 34 of the GDPR.
n) To contribute to the business continuity and disaster recovery planning process.
o) To advise on and monitor the safeguarding of organisational record management, (Retention of Records Procedure.
p) To ensure that records of the processing are kept by Aseptika's as detailed in Article 30 mentioned above.
q) To advise the controller of its obligation to issue privacy notices to data subjects at the point of collection of their personal data under Articles 13 to 15.

4 Management Meetings

4.1 Monthly meetings

- Changes in the environment, which may affect IG (e.g. new contracts, resourcing).
- New risks / update on risk issues.
- Incidents/issues.
- Data quality issues.
- Audits undertaken.
- Privacy Impact Assessments.
- Annual training completion.
- AoB.

Note. Any agenda item for which there is nothing to discuss will be noted accordingly.

4.2 Six monthly meetings

Six monthly meeting (1)	Six monthly meeting (2)
Review • IG Management Framework • IG Policy • Business Continuity Plan • Review any changes required to the Staff IG Handbook • Review user access	• Review asset register. • Review of acceptable risks • Review supplier list. • Data flow mapping • Review adequacy of training arrangements

5 Contractual Requirements for Staff and Third-party Suppliers

Aseptika will ensure that ensures that it fulfils its legal and other responsibilities regarding confidential information is to ensure that all staff members (including temps, locums, students and volunteers) and third-party contractors with access to Aseptika's information or systems are fully informed of their own obligations to comply with information governance requirements for security and privacy.

Aseptika will include a specific and explicit clause in the contract of employment, volunteer agreement or contract for services (e.g. IT services) stating an obligation to keep personal information confidential. Where Aseptika signs up to service agreements (e.g. hosting arrangements), it will ensure that the security and privacy arrangements required are appropriately addressed in the agreement.

The contract will also provide a formal record that Aseptika has taken steps to ensure that staff recognise their own responsibility for protecting health and care information.

Where appropriate an individual or third party will be required sign a non-disclosure agreement.

Breach of confidence, inappropriate use of patient/service user records or abuse of computer systems may lead to disciplinary measures.

Aseptika's policy allows the undertaking of audits of personnel records, contractor and other third-party contracts to determine how many have written contracts, and of those, which contain clauses that identify responsibilities for information governance, linked to disciplinary procedures (where appropriate).

Where any gaps exist, a process should be implemented to ensure that appropriately worded clauses are issued to, signed and incorporated within the contracts of existing staff, contractor and third parties; and all new members of staff and new contracted third parties sign a contract containing an IG clause.

Contracts with 3rd party data recipients must always include a clause requiring incidents to be reported to the data provider.

A copy of the Third-party Non-Disclosure Agreement is available. Key relevant items include:

Key components of third-party non-disclosure agreements
Specific reference to Data Protection and security issues, such as: • Notification of the fact of processing data to the IG Lead. • Obligations to comply with limits set by Aseptika. • The security and data protection standards that apply to both parties. • Whether the contractor can act independently or only on instruction from Aseptika.
Additionally: • Penalties for breach of the non-disclosure agreement. • A provision to indemnify the organisation against breaches by the third party. • Responsibilities for costs, e.g. for security audit, subject access, for handling information requests. • Incident-reporting requirements, contracts with 3rd party data recipients must include a clause requiring incidents to be reported to the data provider.

Our primary security process is not to allow third parties access to any patient-related data unless necessary.

6 Sharing Confidential Information

Data protection law provides conditions that must be met when processing personal information. In addition, where personal information is held in confidence (e.g. details of care and treatment), the common law requires the consent of the individual concerned or some other legal basis before it is used and shared. Staff must be made aware of the right of an individual to restrict how confidential personal information is disclosed and the processes that they need to follow to ensure this right is respected.

Aseptika gains consent from system users for sharing of data (with a healthcare professional) through its applications. Aseptika does not routinely share information for care purposes, except for a contracted service or consented clinical trial or equivalent. This is the systems user's responsibility. If, during training system users on use of the equipment, a staff member has serious concerns on a user's health, the staff member should seek consent from the user to contact a healthcare professional. If the individual is unable to consent through illness or capacity advice should be sought from the Caldicott Guardian. In all circumstances the matter and actions taken should be recorded as an incident.

6.1 Use and Disclosure of Personal Information

Where a care organisation is using and disclosing personal information for purposes relating to the care of an individual the Act will not prevent that use or disclosure. However, other uses or disclosures are likely to require the explicit consent of the individual concerned.

Any queries on sharing personal information must be raised with the Data Protection Officer or another member of the senior management team in the absence of the data protection officer.

See section 10.

6.2 Requests from system users for inform on their records or access to their records

Requests must be directed to the Data Protection Officer.

7 Access Control - See also the Network Security Policy

Aseptika has access control in place, including Aseptika staff access to confidential patient/service user/customer information.

The principle of least access will be adopted for the design and operation of systems to control access to systems and data.

Systems will be designed and configured to support user access controls.

Special attention should be given to managing access rights which allow support staff to override system controls. See ASL IG P-014 Role Access Requirements.

Computer systems have a Login authentication procedure that includes at least a unique user ID and password. The following features will be implemented:

- System/application identifiers will not be displayed until the login procedure has been successfully completed.
- Do not indicate which part of the login information is incorrect, e.g. if a user makes an error. This prevents unauthorised users identifying patterns when attempting to gain access to systems.
- Limit the number of unsuccessful consecutive login attempts. Many systems allow three unsuccessful attempts before locking users out. A pop-up window then advises the user to contact a helpdesk to have the password reset. The system can also be set to record unsuccessful logons (useful to identify frequency of errors and to alert of a possible hacking attempt).
- Limit the maximum time allowed for Login.
- The system should record the date and time of successful logins. Logs may be used during investigations. The log is therefore a valuable source of evidence and should be linked to a workstation identity (see ASL IG F-007 MAC address registry).
- The password being entered should not be displayed in clear text.
- Passwords should not be transmitted in clear text over a network. Passwords should be encrypted through, for example, an RSA or hashing algorithm, for transmission over networks.
- Systems will enforce password changes after a specified period of time.

7.1 Identifying and Authenticating Users

In order to facilitate and operate effective access control and audit functions it should be possible to uniquely identify all users of an information asset. This function may potentially be achieved by unique username and password combination or, in systems containing sensitive information, secondary smart token technology and biometrics.

7.2 Password Management System

Password management systems are used to establish rules concerning the use of passwords in the system. The following criteria will be implemented:

- In all but exceptional circumstances, all users will be identified as individuals (including system administrators) when they Log on.
- Users will have to change their initial password (issued by the system administrator) following their first Log on.
- Web browsers will be configured to configured to prevent the recording of website passwords when logging in to web-based applications. Recording of website passwords renders the password ineffective as a security measure. Passwords are therefore best if manually entered by the user at each login to be effective.
- The system will prevent password re-use.
- Quarterly password changes are enforced, re-use of passwords is prohibited, and passwords must meet the following requirements:

    - ✓ A minimum of eight characters in length.
    - ✓ Differs from the associated username.
    - ✓ Contains no more than two identical characters in a row.
    - ✓ Is not a dictionary word.
    - ✓ Includes both numeric and alphabetic characters.

- Password data will be stored separately from application data.
- Password will be hashed and salted.

7.3 Use of System Utilities

System utilities will be restricted by access control and disabled if not required.

7.4 Session Time Out

Session timeouts will be implemented where possible.

Staff members can access the internet for limited private purposes, e.g. email or web browsing. See the staff handbook (ASL IG P-020 Staff Handbook). The use of web email and the browsing of 'untrusted' web sites may potentially introduce risks, for example, the download of malicious code (spyware, viruses, worms, etc.) or the viewing/sharing of inappropriate or illegal material. Therefore, Aseptika has formal (See the staff handbook (ASL IG P-020 Staff Handbook) policies which detail staff obligations and undertakings for acceptable use.

Aseptika users will acknowledge (digitally, or in writing) 'acceptable terms of use' documentation or similar as part of the registration process. This should explain user rights in unambiguous terms and users should sign to acknowledge they have read, understood and agree to these terms.

User training documentation, guidance and the provision of user training sessions is an integral part of the user registration process.

7.5 Review of User Access Rights

Aseptika user access rights will be subject to regular review.

8 Storage of Personal Information

Aseptika's policy is to hold all client health data in the UK. Software as a service application, which may hold employee data will be subject to risk assessment and mitigation (for example through contract) as required.

9 Ensuring Privacy and Security

Aseptika will ensure that when new processes, services, systems and other information assets are introduced that the implementation does not result in an adverse impact on information quality or a breach of information security, confidentiality or data protection requirements.

A range of activities will be undertaken to fulfil this objective including:

- Undertaking formal privacy impact assessments to ensure that data protection and security issues are identified and mitigated at project/initiative outset. See the privacy impact assessment procedure.
- Mapping and flows and data and ensuring the security of those data flows.
- Deploying encryption in response to assessed risk, contractual, legal or regulatory requirement. See the encryption policy.
- Developing IT systems to ensure data integrity.
- Undertaking development and testing outside of production systems. See ASL IG P-006 Software Test and Release Policy.
- Establishing fall-back arrangement for system and application changes.
- Formal approval of changes to products and system.

10 Transfers of Personal and Sensitive Information

There is a need to ensure that all transfers of personal and sensitive information (correspondence, faxes, email, telephone messages, transfer of patient records and other communications containing personal or sensitive information) are conducted in a secure and confidential manner. This is to ensure that information is not disclosed inappropriately, either by accident or design, whilst it is being transferred or communicated to, within or outside of the organisation.

10.1 Defining Personal and Sensitive Information

Personal Information. This relates to information about a person which would enable that person's identity to be established by one means or another. This might be fairly explicit such as an unusual surname or isolated postcode or items of different information which if taken together could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent.

Sensitive Information. This can be broadly defined as that which if lost or compromised could affect individuals, organisations or the wider community. This is wider than, but includes, information defined as sensitive under the Data Protection Act 1998, e.g. an individual's bank account details are likely to be deemed 'sensitive', as are financial and security information about an organisation.

10.2 Movement of Personal and Sensitive Information

Information is commonly moved around and between organisations, whether in paper health records, in electronic form or on other media. Where this information is personal or sensitive information it must be

transferred with appropriate regard to its security and confidentiality. It is also essential that the media are protected from unauthorised access and environmental damage at all stages of the move. External exchanges should be carried out based on agreements between exchanging organisations.

Procedures and standards to protect information and media (paper, electronic storage media, etc.) in transit will be established (see ASL IG P-017 Data Protection Policy). The business and security implications associated with transferring information electronically, e.g. by email will be considered.

There will also be procedures in place to ensure all personal and sensitive information relating to patients/service users is received to a secure and protected point (ASL IG P-017 Data Protection Policy). These secure points, also referred to as 'safe havens' should be in place wherever the information is received, including transcribing of phone messages, fax in-trays, electronic mailboxes, pigeon-holes and in-trays for paper information etc.

10.2.1 Appropriate Transfer Methods

Guidelines on appropriate transfer and protection measures are provided below under the following headings:

Encryption

Encrypted electronic media transported between sites or organisations should be properly packaged and clearly labelled to ensure they are handled correctly and not corrupted by magnetic fields (ASL IG P-011 Encryption Policy and Procedures).

Email

Email is not a secure system. All staff using email should be made aware of this during their induction training and during any training provided for use of the email system. Therefore, patient identifiable and other sensitive information should not be sent between organisations unless it has been encrypted to standards approved by the NHS.

Email communication directly with clients/patients/service users must only be undertaken with the consent of the client who must be informed that the security of email can be guaranteed.

Emails containing patient identifiable information must be stored appropriately on receipt, e.g. incorporated within the individual's record, and deleted from the email system when no longer needed.

Email attachments are one of the most common methods for transmitting viruses. All users should be informed of the dangers posed by opening attachments, especially those they were not expecting. Up to date anti-malware software that includes anti-virus capability, should be installed and configured where possible for on-access scanning.

10.3 Procedures and Guidance for Staff

Before transferring information, staff should be directed to obtain answers to the following questions:

- Is there a valid need to use/disclose confidential information?
- Is it necessary to use confidential information?
- Has the minimum possible confidential information been used?
- Do the proposed recipients need to know all the confidential information?

- Have all staff members been informed of their responsibilities for protecting confidential information?
- Is the use of confidential information lawful?
- Does the stated purpose for transferring the information make it more important that the information is shared rather than withheld?

Staff should consider:

- How much information can be given, e.g. on the phone?
- Where and how incoming messages are recorded, e.g. a message book?
- When a particular type of mail route may be used, e.g. email.
- When a courier should be used.
- Discussion of patients in public.

All areas from which correspondence, email, telephone messages, transfer of patient records and other communications containing personal information may be sent will be identified and data flows will be assessed for security.

11 Network Operations for Secure Information Communication Technology (ICT) Networks

Aseptika will maintain a network security policy to ensure that access to network and network services are secure. See also the network policy (ASL IG P- 009 Network Security Policy).

11.1 Policy and procedures ensure that mobile computing and teleworking are secure.

Specific requirements for home working are set out in the staff handbook. Remote connection to Aseptika systems, data backup arrangements and system update requirements are set out in the Network Security Policy.

Staff may be required to work in remote locations and should consider the following:

Theft, Loss or Damage of Equipment. Users must not leave equipment in a place where it is vulnerable to theft e.g. unattended in public areas or on the back seat of a car.

Unauthorised Access to Data. Remote workers must lock their screen or close down their system when away from their device. Staff should consider who can view the details on screens and in public locations and use a privacy screen for their device if required.

Encryption**.** Any digital information that is either person identifiable or otherwise sensitive, must be encrypted. This mandate applies to both the storage of, and transfer of any such digitally held information.

Overheard information: Aseptika business should not be discussed in public areas (e.g. trains, cafés) or on remote/client sites where conversations may be overheard by individuals with whom the conversation is not intended.

12 Information Asset Register

Aseptika will maintain registers of all information and information assets, including information, software, physical assets and services including web-based services. Asset registers will identify the asset owners (see ASL IG F-012 Information Assets Register).

13 Physical Security

It is important to ensure that the organisation's assets, premises, equipment, records and other assets including staff are protected by physical security measures. The network security policy (ASL IG P-009 Network Security Policy) identifies the measures taken to protect network equipment/rooms.

13.1 Securing the Premises

All office areas and areas containing IT equipment will have physical access restrictions in place that are appropriate to information/equipment within the area. Staff are responsible for ensuring that physical security measures are maintained, e.g. doors are closed and locked as required.

13.2 Window Security

Windows will be locked risk assessed to determine if blinds or shutter systems are required. Staff are responsible for ensuring that windows are locked (where required) blinds are drawn and main entrance door is looked an office security enabled at the end of the day.

13.3 Alarms

Office premises is protected by burglar and fire alarms which will be regularly tested.

13.4 Keys and Staff Access

Physical keys and access tokens will be issued on a need-to-have basis and logs of issues, returns and lost access keys and security access will be maintained.

13.5 Clear Desk and Clear Screen Policy

Staff are encouraged to clear desks of any sensitive and confidential information when it is no longer required for the task in hand and to ensure that such information is locked securely away overnight. Staff should disable screen savers and should lock their device when the device is left unattended.

13.6 Disposal of paper media

A shredder is provided which must be used for disposal of Aseptika, client or business partner confidential information.

13.7 Assessment of Physical Security

A risk assessment of physical security is undertaken on an annual basis as a minimum. Physical security and risk assess the physical security of its environment.

13.8 Steps to Take Following Unauthorised Access

Any breach of physical security should be recorded as a non-conformity, and a member of the management team should be informed immediately.

14 Business Continuity Plans

Aseptika will maintain business continuity plans to ensure the availability of critical business processes (see ASL IG P-012 Business Continuity Plan).

15 Incident Management and Reporting Procedures

Information incidents include a loss/breach of staff/patient/service user personal data, a breach of confidentiality or other effect on the confidentiality, information security or quality of staff/patient/service user information.

All incidents and near-misses must be reported, recorded and appropriately managed so that where incidents do occur, the damage from them is minimised and lessons are learnt from them. Incidents must be reported via the incident reporting procedure (see ASL IG P-004 Information Incident Reporting Procedure).

16 Risk Management

Risk is managed through organisational change activity, for example undertaking privacy impact assessments and a formal risk management process which assess the risk to information assets using a defined assessment criterion. Risks will be recorded on a risk register (see ASL QM F-710-004 IG Risk Management Record). New risks will be reviewed at monthly management meetings and all existing risks will reviewed on annual basis.

17 Record Quality

Aseptika systems are capture information directly from application users, who are responsible for data correctly. Validation and range checks on data input will be built into applications. Software development and testing will identify integrity issues will be addressed before systems are released to the production environment.

Integrity issues identified by users will be addressed under the incident reporting procedure.

18 Document History

Document History					
Version	Date released for approval	Contributors Initials	Reviewers Initials	Changes from Previous Version	Authorised by
v2.0	12.02.2018	Gareth Lawrence		Major new draft	
V2.1	12.02.2018	KAA		Document Control Page added	

V2.2	14.02.2018	KAA		Formatting	
V2.3	15.02.2018	KAA		Policy number added	
V2.4	16.02.2018	JMA		Updating	
V2.5	28.2.2018	KAA		Updated as Public document	
V2.6	02.05.2018	ETRA	KA	Updating the password management and to a new template	
3.0	11/12/2018	ETRA	KAA, JAA, CB	Annual review and part of CC2018-0187	
4.0	02.12.2019	JA	Kevin Auton /MP	MDR Transition update, part of CC2019-057	
5.0	29.10.2020	JA	MP	Update as per CC2020-059	KAA