Gaddum

Policy Name	Information Governance Framework
Document Created Date	2017
Last Review Date	April 2024
Version	3
Review Period	12 months
Review Date	April 2025
Approved By	SLT

Changes Log:

Change to – page no	**By**	**Date**
Overhaul of policy into new policy template. **Inclusion of Business Support Team function into process.** **Clarification of terminology and processes in relation to evolved systems; e.g. MFA, CRM, Cloud Based Storage Systems**	Ben Whalley	July 2021
Changes to spelling and grammar, removed/edited reference to other policies that no longer exist/incorrectly named	Heather Kerr	March 2023
Review period	Heather Kerr	April 2023
Edits to spelling and grammar	Heather Kerr	April 2024

Gaddum

Contents

Gaddum

1. Purpose of the Information Governance Framework

This framework sets out the procedures, responsibilities, accountability and sanctions that have been put in place within Gaddum to safeguard the movement of personal data.

1.1. Underpinning Procedures

The following procedures included in this framework have been put in place to support the confidential handling of information within Gaddum and the sharing of this information with other organisations:

1.1.1. Confidentiality Code of Conduct: contains clear guidelines on the disclosure of personal information
1.1.2. Safe Transfer of Personal Data Policy: guidelines for sharing data in a lawful manner
1.1.3. Incident Management Procedure: sets out the procedures for responding to a security breach
1.1.4. Business Continuity Plans: setting out procedures for each site in the event of system failure
1.1.5. Data Protection Policy: contains clear guidelines on protecting the rights and privacy of individuals
1.1.6. Access Control Procedure: guidelines to restrict access to personal information
1.1.7. Handling Security Incidents Procedure: outlining the responsibilities of staff and volunteers if a security incident occurs
1.1.8. Record Management Policy: contains guidelines for staff on how to best manage our records

2. Associated Policies

a) Serious and Untoward Incidents Policy
b) Business Continuity Plan
c) Service Operating Procedures
d) Employee Handbook
e) Mobile Working and Equipment Policy
f) Safeguarding Policies
g) Health, Safety and Risk Policy
h) Data Retention and Disposal/Destruction Policy

3. Roles and Responsibilities

3.1. Board

The ultimate responsibility for information governance rests with the Board of Trustees, who ensures there are adequate controls in place at Gaddum.

3.2. Senior Leadership Team (SLT)

Responsible for the day-to-day operation of the charity and ensuring that staff, systems and sub-contractors comply with the requirements of Information Governance. Review all serious incidents involving actual or potential loss of data or breach of confidentiality.

3.3. Information Governance Lead

Provides advice and guidance to managers and staff on information governance, carries out annual audits reviewing compliance, ensures the framework and policies are updated in line with best practice and learning, ensures staff receiving regular training and updates and participates in the investigation and reporting of information incidents.

3.4. Caldicott Guardian

The Caldicott principles have been developed to protect the confidentiality of client information. They are applicable to all identifiable and sensitive client information. The principles are:

a) Justify the purpose(s) for using confidential client information,
b) Only use the confidential information when absolutely necessary,
c) Only use the minimum confidential information that is required,
d) Access should be restricted on a need to know basis,
e) Everyone should be aware of and understand their responsibilities,
f) Use and handling of personal identifiable information should comply with the law.

The Caldicott Guardian within Gaddum is responsible for protecting the confidentiality of personal information and enabling appropriate information sharing. The Caldicott Guardian is the Chief Executive at Gaddum.

3.5. Managers

Managers are responsible for ensuring that their staff understand and comply with their data access levels and information governance policies and procedures. They ensure the asset register has an up-to-date record of which staff are allocated equipment. They approve staff access levels and ensure the compliance of all policies and procedures within the framework.

3.6. Staff

All employees, whether permanent, temporary, contracted, volunteers or third parties are required to sign an Information Governance agreement confirming that they have read and understood the contents of the policies and procedures, and should remain aware of their responsibility and duty to the compliance of these procedures.

This includes maintaining confidentiality of information but also being aware of when it is necessary to disclose confidential information, ensuring secure storage of data and being aware of situations where disclosure may be or may not be required.

3.7. Sub-Contractors and Third Parties

Are required to comply with this framework, associated policies and business-level operational procedures and to report any incidents as required. This forms part of the initial due diligence and service level agreement.

4. Accountability and Responsibility for this Policy

The designated Information Governance Lead in Gaddum is responsible for overseeing day-to-day Information Governance,

a) developing and maintaining policies,
b) standards and guidance,
c) coordinating Information Governance in Gaddum,
d) raising awareness of Information Governance, and
e) ensuring there is ongoing compliance with the policy and its supporting standards and guidelines.

This policy has been approved by SLT and will be reviewed on an annual basis, or when there are changes in legislation relating to Information Governance.

4.1. Sanctions

Breach of this policy could lead to disciplinary action. Following an investigation, it could lead to dismissal depending on the circumstances. See associated Disciplinary Procedure and Employee Handbook.

5. Staff Confidentiality Code of Conduct

Everyone working for Gaddum is under a legal duty to keep clients' personal information confidential (where a serious risk has not been identified). Clients who believe their confidence has been breached may make a complaint to Gaddum and, in addition they could take legal action.

This Staff Confidentiality Code of Conduct has been produced to ensure all staff members at Gaddum are aware of their legal duty to maintain confidentiality, to inform them of the processes in place to protect personal information, and to provide guidance on disclosure obligations.

5.1. Scope

The Code is concerned with protecting personal information about clients, although its content would apply equally to staff and volunteer personal information. Personal information is data in any form (paper, electronic, tape,

verbal, etc.) from which a living individual could be identified, including name, age, address, and personal circumstances, as well as sensitive personal information like race, health, sexuality, etc.

Under the Data Protection Act 2018, the scope also covers genetic, mental, economic, cultural or social identity. Although the Data Protection Act 2018 applies to the personal information of living individuals, this Code also covers information about deceased clients. The Code applies to all staff including permanent, temporary, and locum members of staff.

5.2. Duty of Confidence (Including Duty to Breach Confidence)

A duty of confidence arises out of the common law duty of confidence, employment contracts, and for healthcare professionals, it is part of your professional obligations. The duty of confidence that all Gaddum staff have is to respect the confidentiality of their clients'. Information obtained about their clients' cases may be confidential and must not be used for the benefit of persons not authorized by the client.

Breaches of confidence and inappropriate use of records or computer systems are serious matters which could result in disciplinary proceedings, dismissal and possibly legal prosecution. Therefore, no one is to:

a) Put personal information at risk of unauthorised access,
b) Knowingly misuse any personal information or allow others to do so,
c) Access records or information that you have no legitimate reason to look at this includes records and information about your family, friends, neighbours and acquaintances.

Staff should act as advocates for clients in all matters relating to recording information. Clients can often be powerless and vulnerable, and there is always a power imbalance between staff and clients that must be respected and managed accordingly.

Therefore, staff must be proactive in defending the interests of the clients by protecting their personal information.

Under the common law duty of confidence, identifiable personal information may be disclosed without consent in certain circumstances, these are:

a) Where there is a legal justification for doing so, e.g. to comply with a statute,
b) Where there is a public interest justification - i.e. where the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the client concerned and the broader public interest in the provision of a confidential service,
c) Where there are reasons under safeguarding obligations to do so.

All requests for disclosure of personal information without the consent of the client must be referred too the IG Lead with one exception, that it is believed there to be a significant risk of harm to the individual or others within their care.

5.3. Keep Personal Information Private

Everyone must comply with the following staff guidelines which set out practical things they should do to keep personal information protected:

- **a)** Good record keeping
- **b)** Appropriate use of computer systems
- **c)** Secure use of personal information
- **d)** Reporting information incidents
- **e)** Using secure mobile computing devices

5.4. Disclose with Appropriate Care

Gaddum will ensure that clients are adequately informed about the use and disclosure of their personal information in a 'Data Statement' outlining why, how and for what purpose personal information is collected, recorded and used. The details of this will be available on all of Gaddum sites.

It is each staff member's responsibility to ensure that clients are aware of where they can access this information, and/or that they are provided with an appropriate copy should they be unable to access it online.

Every Gaddum representative must also ensure they are familiar with the information and seek advice from the Information Governance Lead if clients have questions that they are unable to answer.

If authorised to disclose personal information, colleagues must ensure they do so in accordance with the Information Governance Framework and only:

- **a)** Share with those with a legitimate right to see/hear the information,
- **b)** Transfer in accordance with Gaddum's Safe Transfer of Personal Data commitment ,
- **c)** Where possible, disclose the minimum necessary to provide safe care.

If authorised to disclose information that can identify an individual client for non-healthcare purposes (e.g. research, financial audit), this must only be done if:

- **a)** The data subject has given explicit, prior consent and with full understanding of what they are consenting to, or

b) A person authorised to do so has provided explicit, prior consent, in the data subject's best interests and with full understanding of what they are providing consent for.

The above tests are to ensure there is no later dispute about whether consent was given.

6. Safe Transfer of Personal Data Commitment

Gaddum collects information about potential clients and employees as well as those who use services and who we employ. This information is not the property of Gaddum, it belongs to the people that it has been collected from, the data subjects. The organisation is therefore a custodian of this data either as data controller or processor.

As custodians, we are responsible for the safe keeping and security of all information that comes into our keeping.

As a data controller or processor of user information, all representatives of the organisation are responsible for ensuring that client information is handled with care and respect. It is everyone's responsibility to protect this information from those who are not authorised to use or view it. Everyone must ensure they have done everything possible to protect information.

6.1. Requirements for a Secure Location of Confidential Information

Gaddum is on a journey to becoming completely digitised in terms of storage of sensitive and confidential data. However, it is acknowledged that hard copy versions are currently necessary in some circumstances and in these cases:

6.1.1. It should be in an area that is lockable.

6.1.2. The area should be sited in such a way that only authorised staff can enter that location.

6.1.3. If the area is on the ground floor, any windows should have locks on them.

6.1.4. The area should conform to health and safety requirements.

6.1.5. Manual paper records containing personal information should be stored in allocated, locked cabinets when not in use and there should be a plan to digitise any paper records and destroy hard copies as soon as is appropriate.

6.1.6. Computers must not be left on view or accessible to unauthorised staff.

6.1.7. Computers must be locked when a staff member leaves their desk and to be shut down when they leave the site.

6.2. Communication by Post

6.2.1. Written communications containing personal information must be transferred in a sealed envelope and addressed by name to the

designated person within each organisation. They should be clearly marked ‘Private and Confidential – to be opened by recipient only.’

6.2.2. The designated person should be informed that the information has been sent and should make arrangements within their own organisation to ensure that the envelope is delivered to them unopened and that it is received within the expected timescale.

6.2.3. If an organisation has a policy that all mail is to be opened at a central point, this policy must be made clear to all partners. An alternative means of transfer should be arranged where it is essential that the information is restricted to those who have a need to know.

6.2.4. The personal information contained in written transfers should be limited to those details necessary in order for the recipient to carry out their role.

6.3. Communication by Email

6.3.1. The sharing of information within the confines of Gaddum (gaddum.org.uk to gaddum.org.uk email address) does not leave our network and is deemed as secure. However, unnecessarily large amounts of personal data being transferred within this structure should be avoided as best practice, with CRM software the preferred route or point of reference.

6.3.2. The transfer of client personal information by email to a third party (outside of the Gaddum network) is not permitted, unless the information has been encrypted. Microsoft Office products such as Word and Excel have the ability to lock documents with a password. The password to unlock the encrypted document should be sent in a separate email to the recipient.

6.3.3. Where a PDF contains personal information and needs to be emailed, this should be password protected.

6.3.4. If emailing a client, precautions must be taken to include only relevant information regarding the service they are receiving, including only what identifiable information may be necessary (such as first name).

6.3.5. Some services have access to secure systems (such as Egress) in order to share client personal information with third parties. Where these are available and it has been agreed, they must be used.

6.4. Verbal Communication

6.4.1. A considerable amount of information sharing takes place verbally, often on an informal basis. Difficulties can arise because of this informality particularly in open plan offices. Care should be taken to ensure that confidentiality is maintained in such discussions.

6.4.2. If information is to be shared by phone, then steps must be taken to ensure the recipient is properly identified.

6.4.3. Where information is transferred by phone or face-to-face, care must be taken to ensure that personal details are not overheard by other staff who do not 'need to know.' Where possible, such discussions should take place in private locations. Discussions in public places where colleagues can be overheard, and which are involving identifiable information pertaining to data subjects is strictly forbidden.

6.4.4. Messages containing personal information must not be left on answer machines unless a password is required to access them.

6.4.5. Messages containing confidential/sensitive information must never be written on white boards/notice boards even in restricted areas of buildings.

7. Data Protection

This policy highlights the six data protection principles for processing Data under the General Data Protection Regulation (GDPR). It outlines how the organisation adheres to and implements the principles and demonstrates Gaddum's commitment to meet legal obligations as laid down by GDPR and to protecting the individual's data.

7.1. Gaddum will:

7.1.1. ensure that all staff are made aware of their responsibilities to the protection of data through relevant documents and training

7.1.2. regularly review data protection procedures and guidelines within the organisation

7.2. During the recruitment process

The Business Support Team, will ensure that (except where the law permits otherwise):

7.2.1. during the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, e.g. race or ethnic origin, trade union membership or health,

7.2.2. if sensitive personal information is received, e.g. the applicant provides it without being asked for it within his or her CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted,

7.2.3. any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision,

7.2.4. 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages,

7.2.5. health questions will only be asked once an offer of employment has been made.

7.3. During employment

The Business Support Team will process:

7.3.1. health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits,

7.3.2. sensitive personal information for the purposes of equal opportunities monitoring and pay equality review and reporting (if required to report).

7.4. Criminal records information

Criminal records information received by Gaddum would normally not be kept but may be retained in some instances for risk assessment purposes.

7.5. Privacy Notice

Gaddum has produced a Privacy Statement online for clients, which provides information in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This statement outlines the personal information we collect, how it is used and for what purposes.

7.6. Individuals' Rights

Under the General Data Protection Regulations, Individuals have control over the data they supply and how it is used. To ensure you can exercise the rights of the individual correctly, and understand your own rights, please read "Exercising the Rights of the Individual" document.

8. Access Control Procedures

Technical access controls are built into information systems and are monitored by the IT solutions provider. To ensure confidential information is protected, this functionality must be supported by operational and managerial controls put in place by Gaddum.

The Access Control Procedures set out how Gaddum will allocate, manage and remove access rights to computer systems holding client information so that only authorised personnel have access to use and share information held within those systems, and they aim to ensure that access rights are used appropriately by Gaddum staff.

8.1. Scope

These procedures relate to access controls for computer-based information systems managed by Gaddum to store client identifiable data. They therefore cover the allocation, management and removal of user accounts and the guidelines provided to Gaddum staff to ensure they use the service-managed system appropriately.

8.2. Summary of technical access controls

Gaddum utilises Microsoft Windows Active Directory profile management ensuring users only have access rights relevant to the AD Group they are members of. Users are required to login into the domain using a username and password in order to gain access to the server and files. Access to Gaddum server is limited to users located within Gaddum network and the IT provider. Email Access is provided via Microsoft Office 365 E1 plan which is hosted in Microsoft Azure platform. Gaddum also have a number of CRM systems which have associated IG frameworks in relation to their access. Further information can be found with CRM administrators.

8.3. Responsibility for user access management

Gaddum has assigned the Business Systems Manager with the responsibility for determining user access rights to the system. The unnecessary allocation and use of administrator rights is often found to be a major contributing factor to the vulnerability of systems that have been breached, therefore allocation of administrator rights to other staff can only be authorised by the Business Systems Manager with SLT approval.

8.4. General

Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. During their induction to the system each user is given a copy of guidelines for staff on use of the system and their user login details and is required to sign to indicate that they understand that they understand the conditions of access. A record is kept of all users given access to the system.

8.5. New Users

Access is granted on a need-to-use basis and is coordinated by the Business Support Team in partnership with the organisation's IT Solutions Provider. Accounts are suspended immediately when no longer required.

8.6. Change of user requirements

Changes to requirements will normally relate to an alteration to the level of access used or suspension of an account. Situations where an account will be suspended, and passwords change are:

8.6.1. Long term leave, such as;

a) Sabbatical – to ensure that access into that account does not present a vulnerability around data management.

b) Sick leave (extending beyond a two-week period) – to ensure that access into that account does not present a vulnerability around data management. In addition, this is to safeguard the wellbeing of the individual on leave, so that they do not feel pressured to log in to that account.

8.6.2. Alteration to level of access will usually by way of;

a) Secondments externally or to other teams – to restrict access to a need-to-know.

8.7. Password management

The service system has the following password protection features:

8.7.1. Users must change their password after the first log on (having been issued a temporary password that is known to the organisation),
8.7.2. User must select complex passwords (must contain both letters and numbers and be of a sufficient complexity as to not be 'obvious'),
8.7.3. Users must change their passwords periodically at time limits set by the IT system,
8.7.4. Prevention of password re-use,
8.7.5. Multi Factor Authentication,
8.7.6. Users may change their password at their own request.

8.8. Forgotten password

Where a user has forgotten their password, a replacement should be requested from the IT Solutions Provider, who will issue a temporary, single use, password which requires the user to reset their password to one they are more likely to remember.

8.9. Removal of users

As soon as an individual leaves the organisation, all their log ons are revoked. As part of the employee termination process project managers inform their Service Manager of all leavers and their date of leave. This also applies to self-employed contractors.

8.10. Review of access rights

The Business Support Team review all access rights on a regular basis. The review is designed to positively confirm all system users. Any lapsed or unwanted logins, which are identified, are disabled immediately and deleted unless positively reconfirmed. Furthermore, a reflective exercise will be undertaken to identify why these logins were not disabled through other routes.

8.11. Monitoring compliance with access rights

The management of access rights is subject to regular compliance checks to ensure that this procedure is being followed and that service staff are complying with their duty to use their access rights in an appropriate manner.

Areas considered in the compliance include whether:

a) Only staff regularly working in the service are registered as active users on the system,
b) Allocation of administrator rights is restricted,
c) Access rights are regularly reviewed,
d) Staff are appropriately logging out of the service system.

9. Incident Management Procedures

Ensuring personal information remains confidential and secure is everyone's responsibility and therefore, it is important that when incidents do occur, the damage from them is minimised and lessons are learnt.

The Incident Management Procedures set out how Gaddum will investigate and manage information and incidents and provide staff with guidelines on identifying and reporting information incidents, including near misses.

9.1. Scope

The procedures apply to incidents that impact on the security and confidentiality of personal information. These information incidents can be categorised by their effect on clients and their information:

a) Confidentiality,
b) Integrity,
c) Availability.

These procedures apply to all Gaddum representatives.

9.2. Managing Incidents

All service managers have been assigned the role of incident manager for their respective programmes of work, and they will report any incidents to the IG Lead.

Any actual or potential IG Incident in the service will be assigned to one of the following categories and investigated and managed accordingly ensuring that the following steps are taken:

9.3. Client confidentiality has been breached or put at risk

9.3.1. Report that client confidentiality has been breached or put at risk,
9.3.2. Interview the complainant to establish the reason for the complaint and why the practice is being considered responsible,
9.3.3. Investigate according to the information given by the complainant,
9.3.4. Record findings,
9.3.5. Where necessary, provide written explanation to the client with a formal apology if warranted,
9.3.6. Take and document appropriate action.

9.4. Inadequate disposal of confidential material

9.4.1. Investigate how the information left the service by interviewing staff and contractors as appropriate,
9.4.2. Consider the sensitivity of the data and the risk to which the client(s) have been exposed,
9.4.3. Consider whether the client(s) should be informed and, where the breach is likely to result in a risk for the rights and freedoms of individuals effected, Gaddum must by law contact the individuals effected without undue delay,
9.4.4. Record findings,
9.4.5. Take and document appropriate action.

9.5. Attempted or actual theft of equipment and/or access by an unauthorised person

9.5.1. Check the asset register to find out whether equipment is missing,
9.5.2. Investigate whether there has been a legitimate reason for removal of equipment,
9.5.3. If the cause is external inform the police, ask them to investigate and keep them updated with your findings,
9.5.4. Interview staff and check the asset register to establish what data was being held and how sensitive it is,
9.5.5. Establish the reason for the theft/unauthorised access, if possible,
9.5.6. Consider whether there is a future threat to system security,
9.5.7. Inform insurers,
9.5.8. Review the physical security of the organisation.

9.6. If there has been unauthorised access to the network / computer system:

9.6.1. IT provider to conduct an audit to determine whether unauthorised changes have been made to client's records,
9.6.2. Check compliance with access controls procedures
9.6.3. Consider the sensitivity of the data and the risk that it has been tampered with or will be misused, in order to assess whether further action is appropriate,
9.6.4. If computer hardware or the core software has been stolen, inform the system suppliers to enable restoration of system data to new equipment,
9.6.5. Record findings,
9.6.6. Take and document appropriate action.

9.7. Computer misuse by an authorised user

9.7.1. Interview the person reporting the incident to establish the cause for concern,
9.7.2. Establish the facts by:
9.7.3. Asking the system supplier to conduct an audit on activities by the user concerned,

9.7.4. Interviewing the user concerned.
9.7.5. Establish whether there is a justified reason for the alleged computer misuse,
9.7.6. Consider the sensitivity of the data and the risk to which the client(s) have been exposed,
9.7.7. Record findings,
9.7.8. Take and document appropriate action.

9.8. Lost or misfiled client records

9.8.1. Investigate who last used/had the paper record by interviewing staff and contractors as appropriate,
9.8.2. Consider whether any care has been provided based on incorrect information within a client record,
9.8.3. Consider whether client care has been delayed due to information not being available,
9.8.4. Establish whether missing information can be reconstituted e.g., from electronic records,
9.8.5. If information within records has been misfiled, ensure it is restored to correct filing order/returned to correct record,
9.8.6. Where necessary provide a written explanation to the client with a formal apology,
9.8.7. Record findings,
9.8.8. Take and document appropriate action.

9.9. Reporting Incidents

9.9.1. If something that could be considered as an incident has been discovered, it is everyone's responsibility to report it to their line manager and to then complete an incident reporting form. This should then be sent to the Gaddum Information Governance Lead.
9.9.2. In instances where a breach leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, the organisation is obligated to inform the person/persons affected without undue delay (and no more than 72 hours from the discovery of the breach). All incidents must then be reported to the Information Governance Lead who will inform the ICO.
9.9.3. IG Lead will investigate the incident and may need to speak to people involved in identifying and reporting the issue.
9.9.4. All registered incidents are re-evaluated after a 6-month period to assess the effectiveness of the implemented actions in ensuring that either the type of incident is no longer being reported or the volume of those type of incidents has reduced. If there is no change in the volume of each type of incident the senior management are alerted, and appropriate action taken.

10. Handling Security Incidents Procedure

There are several ways in which client confidentiality may be breached such as theft, poor practice and poor disposal of confidential waste. All breaches should be investigated and reported accordingly. This guidance outlines mechanisms for handling security incidents where client confidentiality has been or may have been breached.

The majority of data security breaches are innocent and unintentional such as leaving your computer 'unlocked' when you leave your desk. However, 'near misses' where no actual harm results from the incident, must still be reported and analysed to look for possible ways of preventing an actual incident occurring in the future.

10.1. Definitions

A 'personal data breach' is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

A data security incident could be defined as:

10.1.1. The disclosure of confidential information to any unauthorised individual,
10.1.2. The integrity of the system or data being put at risk,
10.1.3. The availability of the system or information being put at risk,

10.2. An adverse impact can be defined for example as:

10.2.1. A threat to personal safety of privacy,
10.2.2. A legal obligation or penalty,
10.2.3. A financial loss.

If the breach is likely to result in a risk to the rights and freedoms of the individuals effected, Gaddum must by law contact the individuals effected without undue delay, to detail the data breach and outline our next steps with regards to protecting the rights of the individual.

10.3. Types of Security Incidents

The types of security incidents likely to affect client confidentiality are variable. Data security incidents may take many forms including the following:

10.3.1. Theft of equipment holding confidential information e.g., laptops, client files.
10.3.2. Unauthorised access to a building or areas containing unsecured confidential information.
10.3.3. Access to client records by an unauthorised user who has no work requirement to access the records.
10.3.4. Authorised access which is misused.
10.3.5. Electronic access via hacking or viruses.

10.3.6. Misuse of equipment such as the internet on PCs, text messages on mobiles and e-mails.

10.3.7. Inadequate disposal of confidential material e.g., paper, hard drive, laptop or desktop

10.3.8. Car theft/break-ins which may contain a laptop or paper files with confidential data

10.3.9. Unauthorised access to records away from premises (e.g., laptops and client notes.)

10.3.10. Complaint by a client, or a member of the public, that confidentiality has been breached.

10.3.11. Careless talk (for example discussing an individual's case in an open space where people could overhear and identify the individual).

10.4. Data Security Incident Monitoring

A data security incident may come to light because a client has complained about a breach of confidentiality or because of one of the above incidents.

In the first case the cause of the breach will need to be investigated by interviewing the client if possible, interviewing staff and checking incident logs and computer audit trails. There may also be opportunity to investigate CCTV videos.

In the second case the risk to client confidentiality should be assessed and any damage limitation may need to be applied. In cases where a breach of security could lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, it will be appropriate to warn clients of the breach to their confidentiality.

The majority of IT security breaches are innocent and unintentional and would not normally result in disciplinary action being taken.

10.4.1. Incidents should always be investigated immediately whilst there is still the possibility of collecting as much evidence as possible.

10.4.2. Because of the variety of different types of security incident, it is important to have clear procedures in place to cover the main types of incidents. Any investigations may involve a number of key individuals. The investigation should be co-ordinated by the Information Governance Lead, who will decide how to take matters forward/resolve them. All staff should be aware of the need to report any suspicious incidents to the named individual.

10.4.3. Staff must understand the reporting procedures and the type of incidents to report. Near misses are indicators of potential problems and should also be reported. In order to respond fully to an incident, audit logs need to be kept.

10.4.4. A log should be kept of all incidents reported whether they lead to a complaint or not. All incidents should be considered as to whether they indicate a need for improvement in arrangements. The log may be incorporated in other incident logs as appropriate. A regular report on the number, type and location of data security incidents should be made allowing any trends to be picked up and addressed.

10.5. Reporting Arrangements

10.5.1. All incidents or information indicating a suspected or actual data security breach should initially be reported to the IG Lead through line management routes.

10.5.2. A completed incident form should then be sent to the IG Lead, who must keep a record of all incidents that are reported. The record need not be more than a statement of the persons involved in the incident, a description of the incident and what action has been taken. The information incident reporting form is intended to be used for this.

10.5.3. Where the suspected security breach involves the staff members' Service Manager (or in the case of a Service Manager, the Assistant or Head of Department), the individual should inform their Service Manager's superior or when necessary, the Chief Executive.

10.5.4. If a staff member believes a security breach is the result of an action or negligence on behalf of the Chief Executive, the incident should be reported directly to a Trustee. See also Whistleblowing Policy.

10.5.5. Where there has been an incident involving an IT system, the Information Governance Lead and the IT services provider (when necessary) must be informed to determine whether an actual security breach has taken place.

10.5.6. If an actual data breach has occurred, the incident should be reported immediately to the Information Governance Lead.

10.5.7. It may also be necessary to report the incident to others depending on the type of likely consequences of the incident (for example informing the individual if a breach of security could lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed).

10.6. Incident Classifications

10.6.1. Incidents should be classified according to severity of risk, as follows:

1 = High risk of harm to clients whose confidentiality has been breached

2 = Intermediate risk of harm to clients whose confidentiality has been breached

3 = Low risk of harm to clients whose confidentiality has been breached

10.6.2. The Senior Leadership Team in Gaddum should review the number and type of security incidents, which have occurred, regularly and decide on any appropriate preventative action to be taken.

10.7. Procedure for dealing with various types of Incidents

10.7.1. All staff at Gaddum have a responsibility to ensure that their laptops, and PCs are free of confidential information and are not permitted to save files of any format or for any purpose on their allocated Gaddum equipment.

10.7.2. Colleagues must make use of their OneDrive space on the cloud server in order to save documents that could be considered confidential.

10.7.3. Client information must only ever be saved on approved CRM systems and not on local machines.

10.7.4. If there has been a theft of equipment holding confidential information – PCs, laptop, and client notes etc., and unauthorised access to an area with unsecured confidential information:

- **a)** Check the asset register to find out which equipment is missing.
- **b)** Investigate whether there has been a legitimate reason for the removal of the equipment.
- **c)** If the cause is external, inform the Police and ask them to investigate.
- **d)** Interview staff to establish what data was being held and how sensitive it is.
- **e)** Establish the reason for the theft/unauthorised access.
- **f)** Consider the sensitivity of the data and the risk that it will be misused, in order to assess whether further action is appropriate.
- **g)** Consider whether there is a future threat to system security.
- **h)** Inform organisations of replacement requirements, this would be Yellow Grid.
- **i)** Inform system suppliers if appropriate.
- **j)** Follow the reporting arrangements above.

10.7.5. Access to client records by an authorised user who has no work requirement to access the record:

- **a)** Interview the person reporting the incident to establish the cause for concern.
- **b)** Establish the facts.
- **c)** Establish the reason for unauthorised access.
- **d)** Consider the sensitivity of the data and the risk to which the client(s) have been exposed and consider whether the client(s) should be informed.
- **e)** Take appropriate disciplinary action.

f) Follow the reporting arrangements above.

10.7.6. Inadequate disposal of confidential material (paper, PC hard drive)

a) Investigate how the electronic or paper data left the building by interviewing staff and contractors as appropriate.
b) Consider the sensitivity of the data and the risk to which the client(s) have been exposed and consider whether the client(s) should be informed.
c) Take appropriate action to prevent further occurrences.
d) Follow the reporting arrangements above.

10.7.7. Procedure for dealing with complaints about client confidentiality by a member of the public, client or member of staff:

a) Interview the complainant to establish the reason for the complaint and why Gaddum is being considered responsible.
b) Investigate according to the information given by the complainant and take appropriate action.
c) Follow the reporting arrangements above.

11. Record Management

Record management is the responsibility of all Gaddum staff. It is of paramount importance that records are created, handled and stored appropriately as they contain confidential personal information about our clients. The misuse/mishandling of client records is regarded as a data breach and could result in disciplinary and/or legal action.

11.1. Manual / Hard Copy Files containing personal identifiable information

All manual / hard copy files should have a plan to digitise and store securely at the earliest opportunity. Where hard copy files have not yet been digitised:

11.1.1. These must be kept in locked and secure storage. Confidential information should not be left on desks unattended and electronic records should not be left open on computers unattended.
11.1.2. Records should not be removed from the premises unless authorised by the manager of the service, deemed as absolutely necessary and a risk assessment has been undertaken.
11.1.3. Any records that have been authorised to be taken out of the premises must be kept secure at all times and returned to the office as soon as possible. Gaddum will provide lockable bags if required to ensure the records are kept as secure as possible.
11.1.4. If working on public transport, workers should risk assess their surroundings as to the level of confidentially and where possible

ensure that they are not overlooked if working on a laptop, or overhead, if making telephone calls.

11.1.5. Any breaches in record management will be reviewed by the Information Governance Lead and could result in a disciplinary proceeding based on the level of the risk.

11.2. Record Keeping

Records should contain factual material only. No interpretation is to be included, except where it is cited as a reason for a professional decision. In this case, it must be made explicit that it is the professional judgement of the worker, and the evidence should be given for that judgement. For further information and guidance see the service Standard Operating Procedures.

11.3. Recording Information

Recorded material should be kept to a minimum, consistent with accountability and continuity and is set by service Standard Operating Procedures.

11.4. Working for Gaddum at external sites

Where a worker normally operates for Gaddum, but in another professional setting (e.g., Hospital Ward Settings or GP Surgeries) it must be agreed, between the worker, Gaddum manager and the third party, how recordings are to be kept. This will be by way of a data sharing agreement.

Normally the contract between the worker and the client is confidential and will not be recorded on any other records, e.g., medical records. Where for example a GP/another professional is consulted about a matter of medical judgement, risk or legality, a copy of the factual material discussed, advice given, decisions taken and reasons, should be given to the other party to keep for record purposes.

11.5. Open Records Policy

Gaddum operates an ‘open’ records policy and the right of clients to examine all records originating from Gaddum staff relating to them should be borne in mind. Please note that written information originating from a third party cannot be shown to the client without the permission of the third party.

Clients must have the recording policy explained to them on first contact (if it is possible.) They must be made aware at the first opportunity of what information is kept about them, where it is kept, who might see it and their right to see it for themselves.

Please remember that, except in the very clear circumstances where clients have rights and obligations as detailed above, questions about disclosure

and confidentiality can be difficult and staff should seek help and support from their manager or the Information Governance Lead, if necessary.

12. Data Retention and Deletion/Disposal policy

The General Data Protection regulation states that data should not be retained for longer than is necessary for the purpose of which it was obtained. For a full retention schedule and for further information, please refer to the "**Data Retention and Disposal/Destruction Policy**" document.

13. APPENDIX 1: Data Protection Principles of Processing

13.1. The data protection principles of processing:

13.1.1. Processed lawfully, fairly and in a transparent manner
Under the individual's right to be informed, Gaddum will supply information to the individual regarding all of their rights and the processing of their data.

13.1.2. Collected for the specified, explicit and legitimate purpose
Internal documentation will highlight our lawful basis for processing data, and which data we may need to gain consent to process. Any information where consent is our lawful basis must obtain expressed and personal consent form the individual and remain aware that the information should not be processed in future where consent for the processing of this information is withdrawn by the individual.

13.1.3. Adequate, relevant and limited to what is necessary
Through data minimisation, the data requested of an individual will be limited to that which will help with the provision of a service. Some information is required by funders or commissioners where other information may be useful for understanding the individual's situation. All data will have been assessed by the Data & Performance coordinator and each service manager to ensure that data retained is adequate, relevant and necessary.

13.1.4. Accurate and, where necessary, kept up to date
In conjunction with Article 13(2b) of the General Data Protection Regulation, at the time of obtaining personal data Gaddum will inform the individual of their right to rectification, erasure of personal data, the right to restrict processing and to object to processing data as well as the right to data portability.

13.1.5. Retained only for as long as necessary
See Gaddum's Data Retention Policy.

13.1.6. Processed in an appropriate manner to maintain security
Gaddum will have documentation outlining how data is processed for each service ensuring that risks are identified and managed. The safe transfer of data policy highlights the potential risks to data and how we should transfer it securely when working with third parties or providing information to commissioners.

14. APPENDIX 2: Lawful Bases for Processing

14.1. Lawful Bases for Processing

14.1.1. In relation to any processing activity Gaddum will, before the processing starts for the first time (and then regularly while it continues), review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e:

- **a)** that the data subject has consented to the processing,
- **b)** that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract,
- **c)** that the processing is necessary for compliance with a legal obligation to which the organisation is subject,
- **d)** that the processing is necessary for the purposes of legitimate interests of the organisation, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.
- **e)** except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (e.g. safeguarding),
- **f)** document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles,
- **g)** include information about both the purposes of the processing and the lawful basis for it in the relevant privacy notices,
- **h)** where sensitive personal information is processed, also identify a lawful special condition for processing that information, and document it, and
- **i)** where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

14.1.2. When determining whether the organisation's legitimate interests are the most appropriate basis for lawful processing, we will:

- **a)** conduct a Legitimate Interests' Assessment (LIA) and keep a record of it, to ensure that we can justify our decision,
- **b)** if the LIA identifies a significant privacy impact, consider whether we also need to conduct a Data Protection Impact Assessment (DPIA),
- **c)** keep the LIA under review, and repeat it if circumstances change, and
- **d)** include information about the organisation's legitimate interests in our relevant privacy notice(s).

15. APPENDIX 3: Sensitive Personal Information

15.1. Sensitive personal information

Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.

Gaddum may from time to time need to process sensitive personal information. The organisation will only process sensitive personal information if:

15.1.1. The organisation has a lawful basis for doing so as set out in the paragraph above, e.g. it is necessary for the performance of the employment contract, to comply with legal obligations or for the purposes of the Gaddum's legitimate interests, and

15.1.2. one of the special conditions for processing sensitive personal information applies, such as:

- **e)** the data subject (or their legal representative) has given explicit consent,
- **f)** the processing is necessary for the purposes of exercising the employment law rights or obligations of the organisation or the data subject,
- **g)** the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent,
- **h)** processing relates to personal data which are manifestly made public by the data subject,
- **i)** the processing is necessary for the establishment, exercise or defence of legal claims, or
- **j)** the processing is necessary for reasons of substantial public interest.

Before processing any sensitive personal information, staff must notify the IG Lead of the proposed processing, in order that **they** may assess whether the processing complies with the criteria noted above.

15.1.3. Sensitive personal information will not be processed until:

- **a)** an assessment has taken place, and
- **b)** the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

15.1.4. **Gaddum** will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.