# Information Security Policy

**Policy Data Sheet**

| | |
|---|---|
| **Policy Name:** | Information Security Policy |
| **Document Reference:** | BLG154 |
| **Version Number:** | 4 |
| **Ratified By:** | Executive Team |
| **Exec Team Ratified Date:** | 6/10/2015 |
| **Board approval needed?** | No |
| **Board Ratified Date:** | |
| **Review Period:** | 2 years |
| **Review Date:** | January 2022 |

**Contents**


1. Scope of the Policy ..... 2
2. Roles and Responsibilities ..... 2
3. Encryption and Security of Personal Data ..... 3
4. Definition of Personal Data ..... 3
5. Methods for Storage and Transport of Data ..... 4
6. Evaluating if Personal Data should be Transferred ..... 4
7. Email ..... 4
8. Fax ..... 5
   Use of electronic faxing ..... 5
   Use of paper fax machines ..... 5
9. Online Forms ..... 6
10. Use of Cloud Storage ..... 6
11. Online Surveys ..... 6
12. Distribution of Bulk Emails ..... 7
13. Video Conferencing ..... 7
14. Secure File Transfer ..... 7
15. Client and HR Management Systems ..... 7


**ADVICE: Before using this document you should ensure that you have the most up-to-date version. If you are referring to a printed version it may be out-of-date. If in any doubt please check with Human Resources.**

Access to the client and employee management systems ..... 7
Transfer and storage of personal data extracts ..... 7
16. Scanning ..... 8
Scan to email ..... 8
Scan to computer drives ..... 8
17. Storing and Accessing Data Securely ..... 8
Remote storage of data ..... 8
Access to data ..... 8
Local storage of data ..... 8
18. Using Portable Electronic Devices ..... 9
Mobile phones ..... 9
Encrypted memory sticks ..... 9
19. Associated Policies ..... 9
20. Summary of Recommendations ..... 9

## 1. Scope of the Policy

This policy needs to be considered in relation electronic personal information to ensure that it is stored and transported securely. It relates to service users, staff members and volunteers, and enabling appropriate information sharing.

This policy contributes to the Information Governance Framework and is related to a number of associated policies (see Section 18).

This policy is aimed at staff members, volunteers, and 3rd party colleagues working within the group. *Failure to work within this policy will treated as a disciplinary matter and may also lead to a professional governing body being informed if appropriate*.

## 2. Roles and Responsibilities

***Board***

The ultimate responsibility for the security of personal information and its appropriate transport and storage rests with the Board of Directors. The board receives assurance reports from the Clinical and Service Governance Board.

***Caldicott Guardian***

The Caldicott Guardian in The Big Life Group is responsible for protecting the confidentiality of personal information and enabling appropriate information sharing; the guardian is a member of the Board, Clinical and Service Governance Board, and the Executive Team. All staff members, volunteers, and service users must know how to contact the Caldicott Guardian with concerns, or for advice.

***Clinical and Service Governance Board***

Attended by the Information Governance Lead and Caldicott Guardian. Reviews staff training, and reviews all serious incidents involving actual or potential loss of data or breach of confidentiality.

***Executive Team***

Responsible for the day-to-day operation of the group and ensuring that staff, systems and sub contractors comply with the requirements of the Information Security Policy. Responsible for appointing the Information Governance Lead.

***Data Protection Officer/Information Governance Lead***
Provides expert advice to managers and staff on information security requirements for transferring and storing personal data.

***Assistant Director for ICT***
Responsible overall for implementation solutions for transferring and storing personal data. Provides specialist expert advice on solutions for transferring and storing personal data, as required.

***Managers***
Managers are responsible for ensuring that their staff understand and comply with this Information Security policy, and receive appropriate training

***Staff***
All staff members are required to comply with this policy, and undertake training as directed

***Sub contractors and third parties***
Are required to comply with this policy, 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.

## 3. Encryption and Security of Personal Data

Information in both electronic and paper formats is vital to the operation of our business activities and the volume of information we hold is increasing rapidly. To support these activities, we may be required to share information with our commissioners, partners and across the group. As a result of these factors, a number of information requirements are recognised:

- Information needs to be available for our staff to work on in a variety of locations
- information needs to be available for appropriate sharing with partners
- partners' information needs to be shared as necessary with our staff
- data needs to be shared to support impact and performance monitoring internally and externally

As a direct consequence of these needs, there is a corresponding requirement for information to be transported from one location to another. This increasing 'mobility' of information is increasing the risks of loss or unauthorised access to it.

Big Life has solutions which enable us to share information in a controlled manner, to ensure that any personal data is both transported and stored securely, minimising the risks of loss and unauthorised access.

## 4. Definition of Personal Data

Any personal data as defined in General Data Protection Regulations (GDPR) and The Data Protection Act 2018, must be protected by adopting a series of specific measures.

For clarification the definition of personal data, as defined in GDPR is as follows:

> *"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified,*

*directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".*

## 5. Methods for Storage and Transport of Data

This policy outlines the different methods that meet appropriate standards of secure transfer and storage and considers the following:.

- Is the data in transit secure between the sender and recipient?
- Is the data secure if stored during transit?
- How secure is infrastructure used to transport or store the data?
- What controls are in place to manage access to the data?

We should aim to mitigate the risk of transporting personal data by:

- Evaluating the likelihood and impact of potential risks to data
- Implementing appropriate security measures to address the questions above for any solution we use
- Documenting the chosen security measures and, where required, the rationale for adopting those measures
- Maintaining continuous, reasonable, and appropriate security protections.

## 6. Evaluating if Personal Data should be Transferred

Before making the decision to transmit personal data or confidential information electronically, we should first apply the 6 Caldicott principles and identify whether it is appropriate to transfer the data at all:

- Justify the purpose(s) for using confidential information
- Only use confidential information when absolutely necessary
- Use the minimum confidential information that is required
- Access to confidential information should be on a strict need-to-know basis
- Everyone must understand his or her responsibilities
- Understand and comply with the law

We should also be aware of the 7 Data Protection principles for processing data and the Basis for Processing. Refer to the Confidentiality Policy for more information.

## 7. Email

Email is the most insecure way of transferring data and should not, as a rule, be used for transport of personal data.

Secure transport and storage of data is provided when sending emails:

- Using Outlook within RDS, when sending from one Big Life email account to another
- Using NHS.net, when sending email from one NHS.net email address to another NHS.net email address.

However, it is still recommended that alternative methods of transfer are used (See **Secure File Transfer**).

If using email, further security measures should be observed to ensure control over who has access to the recipient's mailbox.

- The document should be password protected:
  - Use good passwords - ones with uppercase and lowercase characters, numbers, spaces, and symbols. A strong password should be at least 8 characters.
  - If you are using password protection for sending files to multiple people, do not use the same password for everyone. Use a different password for each of your recipients.
  - Do not send the password by email
- Ensure that the recipient address is correct – many email programmes auto-suggest previously used email addresses and do not email personal information to email distribution lists
- The recipient should ensure that their computer is secure:
  - Screen locked or log out of RDS, if not using computer
  - Control access to generic mailboxes
  - No use of generic RDS login accounts

## 8. Fax

**General**

The following measures should be adopted when using either electronic faxing or conventional paper fax machines.

- Make sure you check the fax number you are using.
- Check that you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office.
- If the fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine.
- Ring up or email to make sure the whole document has been received safely.
- Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents

**Use of electronic faxing**

When using electronic fax services:

- All incoming faxes should be received into a generic email account which should be regularly monitored and controlled
- Access to the mailbox should be restricted to appropriate staff members
- Any electronic faxes received should not be stored on the local C drive. If there is a need to store the data, this should be within an appropriately restricted folder on the shared I: drive

**Use of paper fax machines**

Use of a conventional paper fax machine is not recommended, but if still to be used, the following measures should be taken:

- Ensure that the fax machine never runs out of paper
- Adopt measures to ensure that incoming faxes are secure

## 9. Online Forms

In the case of online forms where our service users submit data to us through a web based form, a secure form is required, when the data submitted is either personal and sensitive such as:

- ethnic background
- political opinions
- religious beliefs
- health (mental, physical, sexual)
- criminal records

In the case of a simple contact or enquiry form, a secure form s not required. However, users should be advised not to include sensitive information on the contact form.

Data needs to be transported securely once submitted through the online form and kept secure until it is received by the intended recipient Traffic to and from the secure form must be protected using an SSL certificate from a reputable company such as Thawte or Verisign

Storing the data submission from a secure form or fax on the website for collection by the recipient is required. Emailing personal data submitted from an online form to a recipient is completely insecure and solutions using this method are not permitted.
(See **Storing and Accessing Data Securely**)

## 10. Use of Cloud Storage

The requirement to be able to transfer files around the internet has resulted in a move towards cloud storage with a number of well-known service providers, including iCloud, Google Drive, Dropbox and OneDrive.

Cloud providers are likely to store and move data around multiple servers situated in a number of jurisdictions which may very likely be outside the European Economic Area (EEA). This can be a breach of the DPA.

In the case of non personal data, sufficient security measures should be taken to prevent vulnerabilities. We also need to ensure company data is not lost or inaccessible.

Therefore, only team instances of Dropbox for Business should be used for the storage of non personal data. This allows all data storage to be controlled in a central location.

Personal instances of cloud storage providers such as Dropbox should never be used for work purposes.

Files which contain personal data should never be stored or transferred using one of these insecure cloud storage solutions.

## 11. Online Surveys

Online survey provide a method of obtaining data from our staff and users.

Staff should not set up their own online surveys but refer to the Communications team in Group Services.

The product we use is Smartsurvey. This product is registered under the Data Protection Act and all data collected is stored on UK-based servers.

Surveys should ideally be anonymised and not contain data that allows identification of the person submitting the survey.

**ADVICE: Before using this document you should ensure that you have the most up-to-date version. If you are referring to a printed version it may be out-of-date. If in any doubt please check with Human Resources.**

## 12. Distribution of Bulk Emails

When sending out non confidential information to bulk email recipients, where it is important that the recipients are not identifiable by other recipients, Outlook email should not be used to do this.

The product we use is Mailchimp. Businesses wishing to use Mailchimp should contact the Group Communications Team in order to use this solution.

Please note that whilst Mailchimp protects the visibility of the recipient's email address, it is not intended to be used for sending confidential information. Where a file containing personal data needs to be transferred electronically, the Big Life Cryptshare solution should be used.

## 13. Video Conferencing

When using video conferencing internally or externally all users must ensure they have set up meetings in accordance with the Secure Meetings guide.

Users must refer to managers should they wish to use externally with clients or service users to gain authorisation prior to agreeing the meeting. The use of video conferencing for clinical sessions must have prior approval of the Data Protection Officer and the Executive Team.

Users should also refer to the Video Conferencing User and Participant guide.

## 14. Secure File Transfer

A secure file transfer solution is the best method for transferring (sending and receiving) files.

Where a file containing personal data needs to be transferred electronically, the Big Life Cryptshare solution should be used.

## 15. Client and HR Management Systems

As part of our service delivery, it is necessary to store personal data about our clients and employees on various database systems. Whilst it is preferable to keep an electronic rather than paper client record, it is important that the client data is appropriately secured and accessed.

**Access to the client and employee management systems**
Certain principles need to be followed to ensure that data is only accessed by appropriate staff. These include:

- Ensuring that users *must* login to access that data. Generic logins should not be used.
- Ensuring that an appropriate access/role based control policy is in place and that users with access sensitive info are properly granted / revoked access by a named administrator. It should not be possible for someone to sign-up and get access without explicit review.
- In the event that there are limitations to access controls, staff personally responsible for only accessing information on a need to know basis – i.e. for performing a required work-related tasks

**Transfer and storage of personal data extracts**
It is often necessary to run and extract reports from our client and employee management systems in order to report on performance and usage. These reports are often extracted in a PDF or spreadsheet format. Once the report has been extracted, it must be transferred and stored securely. (See **Secure Transfer of Data** and **Storing and Accessing Data Securely**)

## 16. Scanning

**Scan to email**
All multi functional printers have been set up to allow a user to scan a paper document to their email. As this document is sent out from the printer to the internet before being received by the user's email, it should not be used to transmit personal data, unless the document has been encrypted by the scanning solution.

**Scan to computer drives**
Some scanning devices allow documents to be scanned directly to a drive on a personal computer. Scanning of documents containing personal data to the local C drive should only be done as an exception. In this case, the C drive should preferably be encrypted and all data should be removed from the drive by the end of the same working day and stored in an appropriate location on the shared I drive, pending implementation of a more secure solution.

## 17. Storing and Accessing Data Securely

**Remote storage of data**
Where personal data needs to be stored on a website or in a database system, the following considerations should be noted:

- Data should be stored in the database in an encrypted manner. Unencrypted data is available to anyone else with access to the database or its backups.
- The web based user interface for accessing the data must be secure, have strong access controls, and should provide a means for decrypting the encrypted data
- Preferably the website should be on a dedicated and not shared server
- The hosting provider should have adequate continuity, backup, security and access control policies in place
- There should be a detailed audit log available to show details of submissions received and user login access
- All servers and infrastructure used to process and store data should be located in a country where peoples' rights under the UK Data Protection Act are protected

**Access to data**
Certain principles and policies need to be followed to ensure that data is only accessed by appropriate staff. These include:

- Ensuring that sensitive data is never publicly available –users *must* login to access that content. Generic logins should not be used.
- Ensuring that an appropriate access/role based control policy is in place and that users with access sensitive info are properly granted / revoked access by a named administrator. It should not be possible for someone to sign-up and get access without explicit review.
- The database or application must be accessed over a secure connection. In the case of a web based application, SSL must be used (https://). In the case of a client/server based application, the client application should installed on and be accessed over a secure network (e.g. RDS)

**Local storage of data**
If data is taken off the website or out of the database system, it should never be stored on a local C drive. If stored on a shared I drive, appropriate access permissions to that folder should be in place.

If personal data needs to be stored on the local C Drive because of e.g. the use of specialised software, the device's hard drive must be encrypted to secure the data If possible any data stored on the C drive must be moved to the I drive when no longer required.

## 18. Using Portable Electronic Devices

The devices such as USB memory sticks, mobile phones and CDs are particularly vulnerable to loss or theft.

Care must be taken with the use of any portable electronic devices for storage of personal data, as they may not provide adequate protection.

If it is necessary to use a portable electronic device then the data must be securely encrypted or password protected.

Files containing personal data on laptops should never be stored on the local C: Drive unless the drive has been encrypted

Files containing personal data should never be stored on tablets or iPads

**Mobile phones**
All smartphones should be password protected.

After use, the personal information should be securely deleted off the device. It is unacceptable to continue to carry personal information on a portable electronic device beyond the required or necessary time.

Personal devices should only be configured to access Big Life email following authorisation of the IT manager and DPO on the completion of a risk assessment.

**Encrypted memory sticks**
Where personal data needs to be physically transferred from one device to another, an encrypted memory stick should be used. An encrypted memory stick allows information to be stored but renders the information undecipherable unless the correct password is entered.

When transferred, personal data from a memory stick should never be stored on a local drive. It should only be stored in a location with appropriate access permissions on the shared drive. Once transferred, the data should be deleted from the memory stick.

## 19. Associated Policies

- Information Governance Framework
- Keeping Records and Data Protection
- Freedom of Information Act
- IT, Email, Social Networking
- Serious Untoward Incident and Incident
- Safeguarding Children and Young People
- Safeguarding Adults

## 20. Summary of Recommendations

| **Email** |
|---|

- Avoid use of email to send or receive personal or sensitive data outside of Big Life email unless a point to point secure email solution is in place with the partner organisation (e.g. PGP, TLS)
- If sending within Big Life email, use appropriate measures to secure data such as password protecting document
- Preferably use an alternative method such as Cryptshare

**Web**

- Web forms should only be used to receive personal data if they meet the following criteria:
    - The web form is completed over a secure SSL connection (https://) – this means a security certificate must have been applied to the web site where the form is held
    - Where data is stored externally, all data collected from the form should be held in an encrypted format and on servers that are located in a country where peoples' rights under the UK Data Protection Act are protected
    - Data should be retrieved over a secure SSL connection and preferably from within RDS.
    - Retrieved data should not be stored on the local C: drive. If there is a need to store the data, this should be within an appropriately restricted folder on the shared I: drive

**Fax**

- Sending and receiving paper faxes (although insecure) does comply with current data security standards. However care should be taken to secure the paper copy appropriately
- Electronic fax is available and can be used to send and receive faxes securely. Any electronic faxes received should not be stored on the local C drive. If there is a need to store the data, this should be within an appropriately restricted folder on the shared I: drive

**Scanning**

- Scan to email is available on all main multi functional printers. This functionality should not be used to scan in personal or sensitive data unless the document is encrypted and password protected
- If scanning of personal or sensitive data to disk is required, it is only possible to do this to the local C: Drive . In this case, the C drive should preferably be encrypted and all data should be removed from the drive by the end of the same working day and stored in an appropriate location on the shared I: drive.

**File transfer**

- The most secure method to send or receive a file from an external organisation is to use secure file transfer using either the partner's own or our solution Cryptshare (this can be used to transfer filed internally as well)
- Any files downloaded from the secure file transfer site should not be stored on the local C: drive. If there is a need to store the data, this should be within an appropriately restricted folder on the shared I: drive
-

**Online surveys**

- All online surveys are managed through a single secure account on Smartsurvey and must be requested through the Communications Team
- Surveys should ideally be anonymised and not contain data that allows identification of the person submitting the survey

**ADVICE: Before using this document you should ensure that you have the most up-to-date version. If you are referring to a printed version it may be out-of-date. If in any doubt please check with Human Resources.**

**Bulk Email Distribution**

- When sending out non confidential information to bulk email recipients, where it is important that the recipients are not identifiable by other recipients, Outlook email should not be used to do this.
- The product we use is Mailchimp. Businesses wishing to use Mailchimp should contact the Group Communications Team in order to use this solution
- .

**Cloud Storage**

- Files containing personal data should only be stored within RDS within an appropriately restricted folder on the shared I: drive and never be stored or transferred using one of these insecure cloud storage solutions.
- If you need to give external people access to files which don't contain personal data, only team instances of Dropbox for Business This allows all data storage to be controlled in a central location. (The Communications Team can advise)
- Personal instances of cloud storage providers such as Dropbox should never be used for work purposes
-

**Portable Electronic Devices**

- Files containing personal data on laptops should never be stored on the local C: Drive unless the drive has been encrypted
- Files containing personal data should never be stored on tablets or iPads
- All smartphones should be password protected. Any loss or suspected loss should be reported immediately.
- Where personal data needs to be physically transferred from one device to another, an encrypted memory stick should be used. When transferred, personal data from a memory stick should never be stored on a local drive. It should only be stored in a location with appropriate access permissions on the shared I drive. Once transferred, the data should be deleted from the memory stick.