Information Security Policy

Policy Data Sheet

Policy Name:	Information Security Policy
Document Reference:	BLG154
Version Number:	5
Ratified By:	Executive Team
Exec Team Ratified Date:	December 2021
Board approval needed?	No
Board Ratified Date:	
Review Period:	3 years
Review Date:	December 2024

Contents

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 If you are referring to a printed version it may be out-of-date.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.

1. Scope of the Policy

This policy needs to be considered in relation to 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.

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.

Head of IT
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 now used more frequently to transfer data from one person to another.

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

- Using Outlook within Microsoft Office 365 when sending from one Big Life email account to another
- 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, alternative methods of transfer must be used if sending confidential and sensitive data to a individual external to The Big Life Group

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

- If sending information to an external individual and it contains sensitive and confidential data this must be sent via Cryptshare (see **Secure File Transfer)** Alternative methods are sharing data are below.
- If sending a document that contains personal and sensitive information and Cryptshare cannot be used then the document must be sent using password protection:
    - 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.
- 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
- Please ensure you use the blind copy (BCC) option if sending an email to multiple clients
- The recipient should ensure that their computer is secure:
    - If this is internal all staff must ensure their screens are locked or log out of RDS, if not using the computer
    - Control access to generic mailboxes
    - No use of generic RDS login accounts

8. Docmail

Docmail is a web-based hybrid mail solution that is used to send letters to clients in our Mental Health Services. Please refer to the standard operating procedure for your service for details of how Docmail is used.

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 is 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. Staff should use OneDrive and Microsoft Teams as a method of saving and storing information

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.

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 an insecure cloud storage solution.

All staff will have access to their individual BLG one drive accounts, all data will be saved to OneDrive by default on all imaged devices that are enrolled into Azure.

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.

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.

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.

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. Please refer to **Cryptshare Guide (BLG292)**

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.

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

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.

- 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 downloaded from any client management systems (ie reports), this should always be stored within a secure folder within Teams, Onedrive or the Idrive. If stored on a shared I drive or Teams folder, appropriate access permissions to that folder should be in place.

If personal data needs to be stored on the local Drive because of , the use of specialised software for example, staff must use their one drive through Office 365.

USB ports are restricted by default in line with group policy, exceptions on usage can be made by requesting justification of requirement via helpdesk.

18. Using Portable Electronic Devices

The devices such as USB memory sticks and mobile phones 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. If you require a USB then you must arrange for the purchase of an encrypted USB.

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.

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