Information Security Policy

Policy Data Sheet

Policy Name:	Information Security Policy
Document Reference:	BLG154
Version Number:	9
Ratified By:	Executive Team
Exec Team Ratified Date:	May 2025
Board approval needed?	No
Board Ratified Date:	N/A
Review Period:	3 years
Review Date:	May 2028

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 If you are referring to a printed version it may be out-of-date.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

Information Security Policy Statement

We are committed to protecting all our information against any loss of confidentiality, integrity and availability that could impact on our our staff, people who use ours services, finances, operations, legal or contractual obligations or on our reputation. As part of this commitment, we will implement, maintain and continually improve an ISO 27001 compliant information management system.

It is our policy to:-
- To protect all our information assets against loss of confidentiality, integrity or availability.
- Mitigate the risks associated with the theft, loss, misuse, damage or abuse of these assets.
- Ensure that information users are aware of and comply with all current and relevant information security regulations and legislation.
- Provide a safe and secure information system working environment for staff and any other authorised users.
- Make certain that all authorised users understand and comply with this policy and supporting policies and procedures
- Protect the organisation from liability or damage through the misuse of its information.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the information they handle.

We will assess and regularly review all information security risks through our risk assessment process and we will define the necessary controls to mitigate these risks.

We will define information security objectives and improvement actions that are related to this policy and to our information security risks. We will regularly evaluate progress against these objectives through our 'Management Review' process.

We will monitor access to and use of our information in order to establish the effectiveness of our information management system and to identify potential improvements.

Any staff or other authorised user that suspects there has been or is likely to be a breach of information security has a duty to immediately inform a member of management. In the event of a suspected or actual security breach, we may disable or remove any users, data or anything else necessary to secure our information systems.

This policy applies to all employees, visitors, contractors, suppliers and any other parties accessing our information. This policy relates to the use of all our information assets, to all privately owned systems when connected directly or indirectly to our information systems and to all owned and/or licensed software/data.

Any failure to comply with this policy may lead to disciplinary action, including dismissal, or prosecution. In the case of a contractor or supplier failing to comply with this policy, their contract may be cancelled and the contractor or supplier reported to relevant authorities, including the police.

Fay Selvan, CEO

1. Scope of the Policy

This policy sets out The Big Life group's approach to keeping information secure and includes the storage, sharing and transportation of electronic information which The Big Life group holds.

The Big Life group holds a range of Information including:

Public information – information related to The Big Life group which can be viewed by anyone inside or outside of the organisation.

Confidential and/or restricted Information – information including data about the group's staff and volunteers, people accessing our services, and confidential business information

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 Quality Committee.

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.

Quality Committee
Attended by the DPO (Data Protection Officer) 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 theDPO.

Data Protection Officer (DPO)/
Provides expert advice to managers and staff on information security requirements for transferring and storing personal data.

Head of IT / DPO

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. Classification of Data

The Big Life group classifies its data based on its sensitivity, value and criticality to the organisation, to ensure that sensitive corporate and client data can be secured appropriately. The policy sets out acceptable locations for data to be stored, and transmission methods, as outlined in this policy. Further details are available in the Data Classification Policy and Data Classification Record.

4. 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:

5. 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".*

6. 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.

7. 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.

8. 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 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 an 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 of 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, and symbols. A strong password should be at least 12 characters (8 if Multi factor authentication is in place)
    - 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

9. 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.

10. Docman

Docman is a cloud-based platform for managing clinical content within healthcare organisations used by mental health services for sending information to GP practices. Please refer to the standard operating procedure for your service for details of how Docman is used.

11. 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.

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.

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**)

12. 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.

13. Online Surveys

Online surveys 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.

14. 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.

15. Video Appointments and Meetings

Changing workplace practices mean that the use of video applications to carry out appointments and meetings is now commonplace and in some circumstances is the rule rather than the exception. The Big Life group's preferred application for video calls is Microsoft Teams. Video calls (using Teams) should only be conducted using Big Life group devices and the same standards of professionalism should apply as if the sessions was in person.

If there is a need to use Zoom, which has been agreed with the DPO, the web version and not the app must be used.

Users should not conduct calls using unauthorised software such as Skype or Facetime.

Care should be taken that no Personally Identifiable Information is on view during calls eg from Whiteboards, etc and if a suitable space is not available then Microsoft Teams backgrounds should be used.

All relevant policies, including the Keeping Records Policy and the Confidentiality policy, should be adhered to at all times.

Client appointments should not be recorded without consent and then only for training/ supervision purposes.

All users should refer to the Video Conferencing Good Practice Guide for further information.

16. 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 the Cryptshare User Guide for full instructions: User_guide_Cryptshare_web_application.pdf

Big Life School staff transferring children's files must use School2Schools, DfE Sign-in to do this.

17. 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 people. These include:

- Applying multi factor authentication (MFA) or Single Sign On (SSO) to systems and applications where this is an option.
- 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. If a file needs to be saved to One drive or Teams temporarily, in order for it to be shared, it must be deleted as soon as it is no longer needed. (See **Secure Transfer of Data** and **Storing and Accessing Data Securely**)

18. 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.

19. 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.

Local storage of data

If data is downloaded from any client management systems (i.e. reports), this should always be stored within a secure folder within Teams or One drive. If stored on a shared 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. Any data downloaded or stored temporarily must be deleted as soon as it is no longer required.

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

20. Using Portable Electronic Devices

The devices such as 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. For Apple devices
passwords should be a minimum of 8 characters and a combination of letters and numbers
for Android devices passwords should be 8 characters.

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.

21.Visitors to Big Life Group premises

All visitors to Big Life group premises or to Big Life group staff working in premises other than those owned by the group should sign in using the locally agreed procedure.

Planned visits

Where a visit has been planned beforehand, a suitable room should be identified and made available for the meeting to take place. This room should not have any Personally Identifiable Information on view, whether that is on white board, paper or electronic devices. Any electronic devices in the room should be locked or switched off. The path to the identified room should likewise be free of PII.

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.

The person who has arranged the visitor should be available to greet them or have delegated this task to someone who has been given necessary details of visitor name and organisation.

Visitors should be asked for identification and this checked against the expected arrival.

Visitors should be accompanied at all times unless in a public area.

Unplanned visits

Unplanned or unexpected visitors should be asked for their name, the organisation they represent if any, the purpose of their visit and who they wish to see. They should be asked to provide suitable ID.

Unexpected visitors should be asked to wait in a pubic area until it is established that the request to visit is valid and can be accommodated. If this is the case then procedure for planned visits should be followed.

Where it is not possible to accommodate the unplanned visit, whether due to unavailability of staff or rooms or other reasons, then a planned visit should be arranged. If this is not possible the visitor should be asked for contact details so that a visit can be arranged at a later time.

22. Clear Desk and Screen Policy

Staff should ensure the security of information through adapting a clear desk and clear screen policy. When leaving their workspace for any length of time and at the end of the working day staff should:

- Remove from sight all paperwork, notes etc that contain PI and other confidential information
- Essential paperwork should be locked away. As a paperlight organisation any paperwork should be kept to a minimum and kept on a temporary basis only. Once no longer required it should be securely destroyed.
- Ensure that anything sent to printers is collected immediately and processed as needed.
- Ensure that computers, laptops, phones and any other hardware devices are locked and can only be accessed by the device owners using passwords/ MFA. Devices should be switched off at the end of the working day.
- Ensure that laptops and other screens are positioned so that they are not visible to other (unauthorised) people when you are working on them.

These rules apply whether working in BLG premises or working from home.

Associated Policies

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