Data Protection Policy

1. Policy purpose

1.1. The purpose of this policy, and subsequent guidelines is to ensure compliance with the local Data Protection (Jersey) Law (2018), which comes into effect on the 25th May 2018. This policy, and guidelines associated within this policy, replace any previous policies, guidelines or procedures produced by any part of the LV Care Group, pertaining to data protection.

1.2. Under the Data Protection (Jersey) Law (2018), any employee processing data is liable:

1.2.1. to the service user/employee they are processing data about;

1.2.2. for any damage that the service user/employee may suffer as a result of processing which does not comply with the Law.

1.3. Following this policy, and its contained best practice guidelines, is paramount for ensuring compliance with the Data Protection (Jersey) Law (2018).

2. Scope

2.1. The primary purpose for processing data are based on both contractual and legal obligations. In order to keep data safe, this policy is applicable to all employees of all areas of the LV Care Group and its subsidiary companies.

2.2. Adhering to this policy ensures compliance with the Data Protection (Jersey) Law 2018. Adhering to law is a requirement under section 20 of the Nursing and Midwifery Council (2015) (applicable for registered nurses), and the ethos of the Code of Conduct for Healthcare Support Workers and Adult Social Care Workers in Jersey (2015).

2.3. The Fair Processing Notices in appendices e and f have been put together using information available from the Information Governance Alliance (2016), and the Information Commissioner's Office (2018).

3. Definitions

3.1. For the purpose of this policy, and in accordance with the Law, the following definitions apply:

3.1.1. Access Request - An Access Request is when an individual requests to have a copy of the data which is kept about them. Access Requests may be made in writing, or given verbally. Access Requests should be granted using the process in section 11 of this policy.

3.1.2. Authority - The 'Authority' refers to the Office of the Information Commissioner. Their up-to-date contact details are available on their website:

https://dataci.je/contact-us/.

3.1.3. Data - Data is information which is being processed about a living, identifiable person. Data must only be used for the reason that it was collected. Data is recorded as part of a filing system or with the intention that it should form part of a filing system. Data is either personal data, or special data (definitions in 3.1.10 and 3.1.12).

3.1.4. Data subjects - An identified or identifiable, natural, living person, who can be identified, directly or indirectly.

3.1.5. Controller - a Controller is the person who determines the purpose for which data is processed, and how that data is processed. Within the scope of this policy, the manager for each subsidiary company is deemed the Controller for that company.

3.1.6. GDPR - The General Data Protection Regulation (GDPR) is a European wide initiate adopted on the 25th May 2018. Although sitting outside of the European Union, the Channel Islands have their own legislation to ensure the free flow of data between Jersey, Guernsey and the European Union. The United Kingdom will also be adopting the GDPR in May 2018. These laws will be upheld regardless of the outcomes on 'Brexit.'

3.1.7. Healthcare Professional - an individual who is registered with a professional body. Examples include a pharmacist registered with the General Pharmaceutical Council; a nurse registered with the Nursing and Midwifery Council; a doctor registered with the General Medical Council; or a physiotherapists or occupational therapist registered with the Health and Care Professions Council.

3.1.8. Individual - an individual refers to a service user or employee of the LV Care Group or one of its subsidiary companies.

3.1.9. Law - unless stated otherwise, 'Law' refers to the Data Protection (Jersey) Law 2018. This Law is the Jersey equivalent to the GDPR law.

3.1.10. Managers - A manager refers to a manager of within the LV Care Group, or one of its subsidiary companies.

3.1.11. Personal data - Any data relating to a data subject; examples include a person's name, identification number, location data, online identifier.

3.1.12. Processing - Processing data refers to any operations being performed with personal data. This may include collecting, using, storing and disposing of the data.

3.1.13. Special data - Special data is includes the ethnicity, race, political views, religious and/or philosophical beliefs, trade union membership, genetic/biometric data, health data, sexual orientation, confirmed/alleged criminal record of a living and identifiable person.

4. Six Principles of GDPR

4.1. The GDPR states the following principles must be applied when processing personal data:

4.1.1. Data must be processed lawfully, fairly and in a transparent manner in relation

to the data;

4.1.2. Data must be collected for specified, explicit and legitimate purposes and once collected, not further processed in a manner incompatible with those purposes;

4.1.3. Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4.1.4. Data must be accurate and, where necessary, kept up to date, with reasonable steps being taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

4.1.5. Data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed; and

4.1.6. Data must be processed in a manner that ensures appropriate security of the data, including protection against accidental loss, destruction or damage, using appropriate technical or organisational measures,

(Data Protection (Jersey) Law 2018).

5. Duties of the Compliance Manager

5.1. The Compliance Manager is responsible for ensuring that:

5.1.1. This policy and its subsequent guidelines are kept up-to-date;

5.1.2. Auditing compliance with the Law and this policy;

5.1.3. Provide advice for carrying out Data Protection Impact Assessments;

5.1.4. Must co-operate with any requests/orders of the Authority;

5.1.5. Have overall responsibility for the Information Asset Register.

5.2. The Compliance Manager acts as the Data Protection Lead for the company. LV Care Group does not have a Data Protection Officer. This is because the LV Care Group is not a public authority, and does not process data on a large scale.

6. Duties of Controllers

6.1. So as to be compliant with the Law, Controllers must carry out the following duties:

6.1.1. Be registered with the Office of the Information Commissioner (without registration, the Controller cannot process data);

6.1.2. Be compliant with the data protection principles described in section 4;

6.1.3. Must ensure appropriate safeguards are in place when processing personal data (see section 18: Best Practice Guidelines);

6.1.4. Where a processor is appointed, must appoint a processor in accordance with paragraph 7.1;

6.1.5. Must report any personal data breach in accordance with section 12;

6.1.6. Must co-operate with any requests/orders of the Authority;

6.1.7. Must liaise with the Compliance Manager to keep the Information Asset Register up-to-date;

6.1.8. Must notify the Compliance Manager when a new computer system/process is introduced, so as the appropriate Data Protection Impact Assessment can be

undertaken.

7. Duties of processors

7.1. Processors who are appointed, must have a Code of Conduct, a contract, or certification of GDPR compliance which they can evidence;

7.2. A Processor must be registered under Law in order to process data;

7.3. As with Controllers, Processors have a responsibility to implement measures against unauthorised/unlawful processing of data and accidental destruction/damage of data. Technical measures include:

- 7.3.1. Using pseudonyms as appropriate;
- 7.3.2. Encrypting personal data;
- 7.3.3. Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- 7.3.4. In the event of a physical or technical incident, the Processor must have the ability to restore the availability and access to personal data in a timely manner;
- 7.3.5. Regularly testing, assessing and evaluating the effectiveness of measures to ensure security of processing;
- 7.3.6. Keeping records of the processing activity of the data;
- 7.3.7. Co-operating with a request/order from the Authority.

7.4. Contracts only need to be in place with data processors, not organisations who act as data controllers in their own right.

8. Transfer of information

8.1. In order to provide appropriate care, and employment terms, it is often necessary to share information with other professional bodies. These organisations may be private or public bodies.

8.2. All employees and service users must sign a Fair Processing Notice, demonstrating that they understand the necessity of transferring such information.

- 8.2.1. Employees and service users must understand that they have the right to withdraw their consent for data sharing at any point. However, withdrawing consent may have an impact on their care/employment.

8.3. Any information transferred must be done appropriately. This means:

- 8.3.1. Only sharing the necessary information;
- 8.3.2. Ensuring that the information is transferred as safely as possible.

9. Data Protection Impact Assessments

9.1. Data Protection Impact Assessments (DPIAs) are to be used either when:

- 9.1.1. New technology is being introduced which will handle/process data;
- 9.1.2. The data being processed carries high risk.

9.2. This is to ensure that using the proposed system complies with internal data protection policies and best practice.

9.3. Managers proposing to implement new systems must liaise with the Compliance Manager to undertake the Data Protection Impact Assessment (figure 1). The form is available in appendix g.

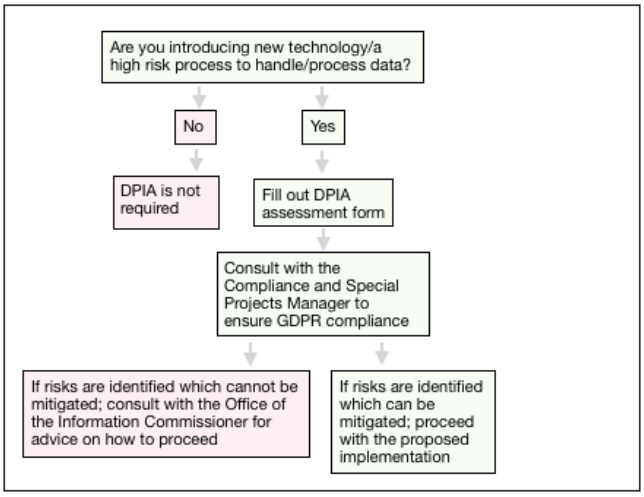


Figure 1: Flowchart for determining the need for a Data Protection Impact Assessment

10. Information Asset Register

10.1. LV Care Group has a responsibility to have an up-to-date Information Asset Register.

10.2. The purpose of the register is to hold an up-to-date listing of the data held within the LV Care Group, including its subsidiary companyes.

10.3. The Compliance Manager will arrange for the Information Asset Register to be updated on a quarterly schedule.

10.4. Managers have a responsibility to liaise with the Compliance Manager if there are changes to their Information Assets between these times.

11. Rights of data subjects

11.1. The individual has the right to be informed by a Controller if their personal data is being processed by/on behalf of the Controller.

11.2. Regarding information given, individuals have the right to know:

- 11.2.1. Why their information is being/going to be processed;
- 11.2.2. The categories of personal data concerned;
- 11.2.3. Who the information will be given too;
- 11.2.4. How long the information will be stored for;
- 11.2.5. The individual's right to ask the Controller to rectify/erase/restrict the processing of their data;
- 11.2.6. Their right to lodge a complaint with the Authority;

11.3. In situations where data cannot be obtained from an individual, the information source must be documented.

11.4. Right to access health records

11.4.1. A Controller who is not a healthcare professional must not refuse an Access Request.

11.4.2. A Controller who is not a healthcare professional must not give out information in health records as part of an Access Request, unless they have consulted with a healthcare professional prior to releasing information. Managers must liaise with the Compliance Manager for guidance prior to giving out information held in health records.

11.4.3. For the purpose of this policy, health records include but are not limited too, documents signed written by a nurse, healthcare assistant, General Practitioner, pharmacists or medics.

11.5. Right for rectification

11.5.1. The individual has the right to ask the data Controller to amend data held about them, stating the inaccuracy, and/or explaining incomplete data, along with the required changes.

11.5.2. The data Controller may request reasonable proof/information in order to verify changes to data held about an individual. This will ensure accuracy of changes to data held. Once this verification has occurred, the Controller can rectify/complete the data.

11.5.3. If it is unreasonable to confirm/verify/complete data; the Controller who is taking the data must write a record that the client/resident disputes accuracy/completeness of the data. The data Controller can request, in writing, the information needed in order to rectify/complete the data.

11.6. Right for erasure

11.6.1. In the following circumstances, the Controller must erase an individual's information (so long as this request is not superseded by a retention schedule):

11.6.1.1. The data is no longer necessary in relation to its original collection;

11.6.1.2. The individual withdraws consent (as long as there are no other legal grounds for processing the data);

11.6.1.3. Data has been unlawfully processed;

11.6.1.4. Compliance with a legal obligation;

11.6.1.5. Data was collected relating to a child who was unable to give valid consent.

11.6.2. If data is within the public domain and an individual asks for their data to be erased, the Controller must take reasonable steps to inform other data Controllers involved with processing that data.

11.6.3. This right does not apply in instances of freedom of expression and/or information, legal compliance, in the interest of public health, archiving and research, or the defence of legal claims.

11.6.4. Records must be kept for the detailed retention period, detailed in section 17.

11.7. Right to restriction of processing

11.7.1. The individual has the right to obtain Controller restriction of processing in one of the following:

11.7.1.1. The individual states that the data held about them is not clear. Whilst verifying the accuracy of the data, the data must not be processed;

11.7.1.2. Processing is unlawful and the individual does not want their data erased, instead requesting restriction;

11.7.1.3. The Controller no longer needs data for processing, but requires for the purposes of establishing/ exercising/ defence in legal claims;

11.7.1.4. The individual does not want their data processed for public functions/legalities whilst waiting to verify if legitimate grounds/reasons of public interest that the Controller can override;

11.7.2. If processing is restricted due to any of the above, excluding storage, data can only be processed:

11.7.2.1. With the individual's consent;

11.7.2.2. For the purposes of legal proceedings;

11.7.2.3. For vital interests;

11.7.2.4. In the case of public interest.

11.7.3. The Controller must inform the individual prior to lifting the restrictions of processing.

11.8. Right to data portability

11.8.1. When processing is automated (i.e carried out by a machine which does not require/requires very little human input), the individual has the right to receive personal data which they have given to the Controller in a structured, machine-readable format.

11.8.2. The individual can ask for automated data to be transmitted to another Controller, where it is feasible and without hindrance from the Controller to which the personal data was provided originally provided.

11.8.3. Where exercising the individual's right to data portability, the individual has the right to have personal data transmitted directly from one Controller to another, where technically feasible.

11.8.4. This right does not apply when the rights/freedoms of others may be adversely affected.

11.9. Right to object to processing for the purpose of public functions or legitimate interests

11.9.1. The individual has the right to object to processing.

11.9.2. In such an instance, the Controller must notify the individual of the processing functions and the right to object. Such a notification must be at the Controller's first communication with the individual, must be explicit, and separate from other matters.

11.9.3. Processing must be stopped if the individual objects; the exception would be if the processing is occuring for legitimate/reasons of public interest.

11.10. Right to object to processing for direct marketing purposes

11.10.1. The individual has a right to object to data processing related to marketing, and the individual must be made aware of this right.

11.10.2. Data must be gained at the Controller's first communication with the individual, must be explicit, and separate from other matters.

12. Procedure for breach in the Regulation

12.1. Data breaches must be reported to the Data Controller and the Compliance Manager as soon as possible of the breach being discovered. Depending on the severity of the breach, it may be necessary to refer the breach to the Authority.

12.1.1. If breaches are not reported to the Authority, an internal investigation must take place in order to ascertain risk and prevent a similar occurrence in the future. The breach must be logged and investigation documented.

12.1.2. In the instance that breaches are found out-of-hours, the Compliance Manager must be notified. Should the Compliance Manager not be available (i.e. annual leave), a suitable contact will be appointed and this information will be distributed.

12.2. All breaches must being reported to the Authority must be reported to the Authority within 72 hours of becoming aware of the breach, using the form in appendix c. The notification of the breach must be made in writing and must:

12.2.1. Describe the nature of the personal data breach. This includes the categories of data which has been breached, and the approximate number of data subjects affected, along with the number and categories of personal data records concerned;

12.2.2. Include the name and contact details of the Compliance Manager where further information can be obtained;

12.2.3. Describe the likely/potential consequences of the data breach;

12.2.4. Describe the measures taken/proposed in order to address the personal data breach. Where possible, this should include measures to mitigate potential adverse effects.

12.3. If the Authority is notified after 72 hours, the notification must be accompanied with reasons for the delay.

12.3.1. Information must not be delayed being given to the Authority because all of the information is not available in the first instance. It is acceptable to provide the information in phases so as to prevent undue delay in proceedings.

12.4. The Controller must factually document personal data breaches in detail for investigation by the Authority.

12.5. If the data breach is likely to be high risk to the rights and freedoms of an individual, the Controller must inform the individual of the breach;

12.5.1. As soon as is practicably possible;

12.5.2. In clear and plain language;

12.5.3. With a description of the nature of the breach;

12.5.4. With the likely/potential consequences of the data breach;

12.5.5. And describe the measures taken/proposed in order to address the personal data breach. Where possible, this should include measures to mitigate potential adverse effects.

12.6. Exceptions to informing the individual include:

12.6.1. Where the information is unintelligible to anyone without sufficient authorisation, i.e. encrypted data;

12.6.2. The Controller has taken measures to ensure that the high risk to the rights and freedoms of data subjects are not likely to occur;

12.6.3. A disproportionate effort would be required. In this case, the Controller will need to consider measures such as public communication so as individuals are informed in an equally effective manner.

12.7. When reporting a breach, it must be considered whether or not the Jersey Financial Services Commission must also be informed.

12.7.1. In such a situation, the Office of the Information Commissioner should be sought for advice.

13. Access requests

13.1. Access requests will be dealt with by the Data Controller, and will be followed up within 4 weeks of receipt of the request. If a request is complex in nature, then the request period can be extended by a further 8 weeks. The Data Controller must inform the data subject if an extension beyond the original 4 weeks is going to occur, along with reasons for the delay.

13.2. If the request is made via electronic means, the reply should also be via electronic means.

13.3. Ordinarily, clients/residents must not be charged for access requests.

13.4. Should a client/resident make requests which are unfounded or excessive, the Controller has the right to either refuse or charge a fee to cover the administrative costs of providing the information.

13.5. Access requests cannot limit the rights/freedoms of others, but otherwise service users have the right to information about them and a copy of this data. Regard must be considered for the confidentiality and capacity of any other individual who may be referred to within the data being sought. In such a circumstance where someone else's data is involved within the data being requested, that individual has the right to refuse data regarding them being divulged in an access request.

13.6. First copies of access requests are free of charge, however further copies can be charged in order to cover administration costs. This only applies to copies of the same access requests. A subsequent access request for different information will be free of charge as it constitutes as a new request.

14. Training

14.1. All employees must attend data protection training annually. Training requirements are stipulated in appendix d.

14.2. The company will ensure that training is available; however it is the responsibility of the individual employee that they attend such training.

14.3. The Training Manager is responsible for keeping up-to-date records about employees who are in-date with their training. Records will be shared with the relevant managers for employee's personal training records. Relevant training records will be made available for auditing purposes.

14.4. Managers are responsible for ensuring that employees are able to access the provided training. If managers arrange a time for employees to attend training and the employee cancels for any reason, it is the responsibility of the employee to arrange time to attend their own training.

15. Data Audits

15.1.1. Data Audits will be undertaken annually.

15.1.1.1. This schedule may be more frequent, if this is deemed appropriate by management.

15.1.2. Actions from the audits will ensure that information regarding data entry, flow and exit from the organisation is up-to-date.

15.1.3. Managers have a responsibility to liaise with the Compliance Manager, if there are changes to their data flows in the meantime.

16. Fair Processing Notices

16.1. Fair Processing Notices ensure that employees and service users understand their rights for their data being used by us.

16.2. Appendix e is the Fair Processing Notice for service users, and every service user must have signed one of these Notices. The signed Notice will be kept with the service user's records. The admitting employee has the responsibility to ensure that this Notice is signed on admission/commencement of service. Managers also have the responsibility to ensure that this Notice has been signed.

16.3. Appendix f is the Fair Processing Notice for employees. Every employee must sign one of these notices. The signed Notice will be kept in the employee's records. The hiring manager has the responsibility to ensure that their employees have signed this Notice.

17. Recruitment

17.1. Information from unsuccessful job applicants is to be destroyed via shredding after 3 months. No information is to be kept longer than 6 months. This includes any information gained from criminal record checks (ICO, 2011).

17.1.1. If there is a need to keep it longer, this must be justified and documented. The documented rationale is to be kept with the applicant information.

17.2. Job applicants must be advised as early as possible that their data will be processed for the recruitment process.

17.3. Successful job applicants must sign a Fair Processing Notice for employees. This can be done at the same time as signing a job contract.

18. Post-employment

18.1. Upon leaving employment with LV Care Group, the manager has a responsibility to ensure that company information is not taken away from the company.

18.1.1. If employees use their own devices, they need to be prepared to have company data deleted from their devices/home systems.

18.1.2. Upon termination of employment, all information, devices and passwords provided by the company must be returned to the company.

19. Retention schedules

19.1. Data must be kept in accordance with the following data retention schedule (Information Governance Alliance, 2016).

Data type	Retention trigger	Review date	Action at the end of the retention period
Adult health records/social records	Discharge or patient last seen	20 years from last entry, or 8 years from passing away (only if they died whilst receiving organisational services)	Review, and appropriately destroy if no longer needed
Children's health records	Discharge or patient last seen	25th birthday, or 26th birthday if the child receives treatment when they are 17 years old	Review, and appropriately destroy if no longer needed
Mental health records	Discharge or patient last seen	20 years, or 8 years after patient has died, whichever is soonest (only if they died whilst receiving organisational services)	Review, and appropriately destroy if no longer needed
Record of long term illness	Discharge or patient last seen	30 years, or 8 years after patient has died, whichever is soonest (only if they died whilst receiving organisational services)	Review, and appropriately destroy if no longer needed
Serious incidents	Serious incident case closed	20 years	Review, and transfer information to place of deposit
Non-serious incidents	Incident case closed	10 years	Review, and transfer information to place of deposit
Polices	Creation	Life of the organisation + 6 years	Review, and transfer information to place of deposit
Occupational health records	Employee leaves	75th birthday, or 6 years after employment has ceased, whichever is soonest	Review, and appropriately destroy if no longer needed
Employee records (including clinical training records)	Employee leaves	75th birthday, or 6 years after employment has ceased, whichever is soonest. Mandatory training records	Review, and appropriately destroy if no longer needed

		must be kept for 10 years after training is completed. All other training records must be kept for 6 years from when the training was completed.	
Timesheets	Creation	2 years	Review, and appropriately destroy if no longer needed
Complaints	Closure of incident	10 years	Review, and appropriately destroy if no longer needed
Access Request	Closure of SAR	3 years	Review, and appropriately destroy if no longer needed
Access Request, with appeal	Closure of appeal	6 years	Review, and appropriately destroy if no longer needed
Pharmacy Records	Refer to Pharmacy Policies		

20. Best practice guidelines for implementing the GDPR

As an employee of LV Care Group, or one of its subsidiary companies, you must:

- Access GDPR training annually. Attendance is recorded and is mandatory.
- Only collect data which is relevant for the individual at that point in time.
- Never store personal data about a client/resident on a personal laptop/device.
- Not send personal data via email. The only exception is when appropriate measures are in place. If information is password protected, the password should be given via another form of communication, i.e. verbal/text message.
- Lock computers which have personal data on them, when the computer is unsupervised.
- Not leave personal data unsupervised on a desk.
- Dispose of paperwork with personal data on by shredding it. If a shredder is not available, the paper for shredding must be disposed of in a secure container which is allocated for shredding.
- Ensure that all personal data is locked away (i.e. in a filing cabinet), and the keys stored in a safe place.
- Transport data in as safe a manner as possible. This means only transporting a laptop/device containing personal data if the data is encrypted. The laptop/device should be transferred in a lockable case. If travelling in a car, best practice is to put data in the boot of a car, away from where the data may be seen. If possible, multiple files pertaining to one service user must not be transferred at the same time.
- Keep your passwords for company computers, emails and/or documents safe. You must change them regularly and not share them with anyone. This includes colleagues within the company.
- Accompany visitors in Company areas which are normally restricted to employee/where personal data is stored.
- Ensure that computer screens are positioned where they cannot be accidentally read, i.e. not having the screen face a window/mirror.
- Ensure that digital information is backed-up in a secure manner.
- Not release client/residential data without their consent. If data is being requested for legal proceedings, you must refer to your line manager.
- Check the identity of people asking for the data of clients/residents.
- Limit the amount of information given out over the telephone.
- Refer all Access Requests to the relevant line manager immediately to appropriately dealt with.
- Advise clients of the necessity of keeping their data in a secure location.
- Notify your line manager immediately of any data breaches. All data breaches must be reported to the regulatory authority within 72 hours of the breach being discovered. Appendix c in the policy details the information needed and who this information should be sent too.
- Comply with internal data protection audits.
- Only give personal data to other agencies, with the client/resident's permission, and record this conversation in their notes.

21. Consultation and ratification schedule

Name and position	Date consulted
Nick Bettany - Director	April 2018
Chris Shelton - Director	April 2018
Edgar Dingle - Director of Community Care	April 2018
Matt Johnson - Director of Pharmacy and Community Care	April 2018
Kathy Murphy - Manager for Lavender Villa Residential Home	April 2018
Maggie Stobart - Manager for Cheval Roc Nursing and Residential Home	April 2018
Noel Leonard - Manager for Rosemary Cottage	April 2018

Date ratified	30th April 2018

22. Reference list

Data Protection (Jersey) Law 2018, Jersey. Available at: https://www.jerseylaw.je/laws/enacted/Pages/L-03-2018.aspx. (Accessed: 3rd April 2018).

Data Protection Authority (Jersey) Law 2018, Jersey. Available at: https://www.jerseylaw.je/laws/enacted/Pages/L-04-2018.aspx. (Accessed: 5th April 2018).

Information Commissioner's Office (2011). 'Employment practices code of practice,' Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/employment/. (Accessed: 14th May 2018).

Information Governance Alliance (2016). 'Records Management Code of Practice for Health and Social Care,' Available at: https://digital.nhs.uk/records-management-code-of-practice-for-health-and-social-care-2016. (Accessed: 11th April 2018).

Nursing and Midwifery Council (2015). 'The Code Professional standards of practice and behaviour for nurses and midwives,' Available at: https://www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/nmc-code.pdf. (Accessed: 5th April 2018).

States of Jersey (2015). 'Code of Conduct for Healthcare Support Workers and Adult Social Care Workers in Jersey,' Available at: https://search3.openobjects.com/mediamanager/jersey/asch/files/code_of_conduct_booklet_pdf_version.pdf. (Accessed: 5th April 2018).

23. Bibliography

Information Commissioner's Office (2016). 'Training checklist for small and medium sized organisations,' Available at: https://ico.org.uk/media/for-organisations/documents/1606/training-checklist.pdf. (Accessed: 6th April 2018).

Information Commissioner's Office (2018). 'Good and bad examples of privacy notices,' Available at: https://ico.org.uk/media/for-organisations/documents/1625136/good-and-bad-examples-of-privacy-notices.pdf. (Accessed: 11th April 2018).

Information Governance Alliance (2018). 'The General Data Protection Regulation: Implementation Checklist,' Available at: https://digital.nhs.uk/media/35500/IGA-GDPR-Implementation-Checklist-V1-FINAL/pdf/IGA_-_GDPR_Implementation_Checklist_V1_FINAL. (Accessed: 6 April 2018).

Appendix a - Guidelines for employees

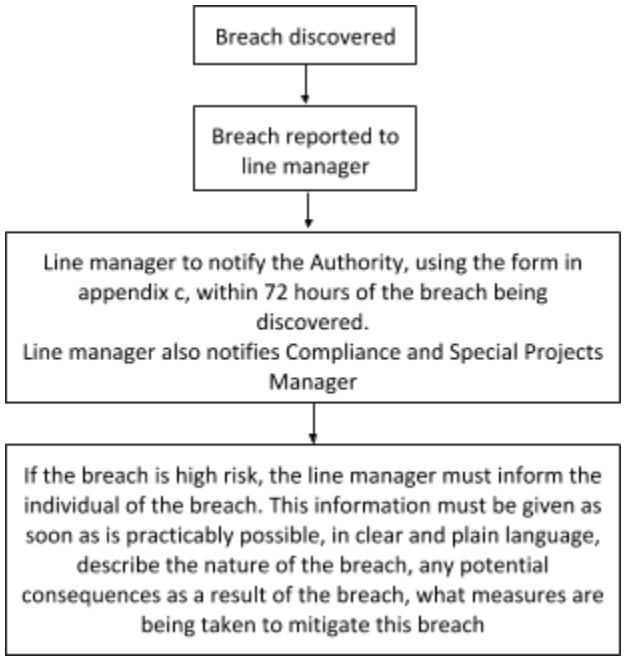
The new Data Protection Law will be used from the 25th May 2018. This new law (also referred to as the General Data Protection Regulation or GDPR) replaces the previous Data Protection (Jersey) Law 2005.

As an employee of LV Care Group, or one of its subsidiary companies, you must:

- Access GDPR training annually. Attendance is recorded and is mandatory.
- Only collect data which is relevant for the individual at that point in time.
- Never store personal data about a client/resident on a personal laptop/device.
- Not send personal data via email. The only exception is when appropriate measures are in place. If information is password protected, the password should be given via another form of communication, i.e. verbal/text message.
- Lock computers which have personal data on them, when the computer is unsupervised.
- Not leave personal data unsupervised on a desk.
- Dispose of paperwork with personal data on by shredding it. If a shredder is not available, the paper for shredding must be disposed of in a secure container which is allocated for shredding.
- Ensure that all personal data is locked away (i.e. in a filing cabinet), and the keys stored in a safe place.
- Transport data in as safe a manner as possible. This means only transporting a laptop/device containing personal data if the data is encrypted. The laptop/device should be transferred in a lockable case. If travelling in a car, best practice is to put data in the boot of a car, away from where the data may be seen. If possible, multiple files pertaining to one service user must not be transferred at the same time.
- Keep your passwords for company computers, emails and/or documents safe. You must change them regularly and not share them with anyone. This includes colleagues within the company.
- Accompany visitors in Company areas which are normally restricted to employee/where personal data is stored.
- Ensure that computer screens are positioned where they cannot be accidentally read, i.e. not having the screen face a window/mirror.
- Ensure that digital information is backed-up in a secure manner.
- Not release client/residential data without their consent. If data is being requested for legal proceedings, you must refer to your line manager.
- Check the identity of people asking for the data of clients/residents.
- Limit the amount of information given out over the telephone.
- Refer all Access Requests to the relevant line manager immediately to appropriately dealt with.
- Advise clients of the necessity of keeping their data in a secure location.
- Notify your line manager immediately of any data breaches. All data breaches must be reported to the regulatory authority within 72 hours of the breach being discovered. Appendix c in the policy details the information needed and who this information should be sent too.

- Comply with internal data protection audits.
- Only give personal data to other agencies, with the client/resident's permission, and record this conversation in their notes.

Appendix b - Flowchart for managing breaches in data protection



Appendix c - Data Breach notification form

Box 1
Name: **Designation:** **Work address:** **Contact telephone number:**
Box 2
Date and time that you were notified of the data breach:
Box 3
Describe the nature of the personal breach: *(Include details of the categories of the data breached, the approximate number of data subjects affected, the number and categories of personal data records concerned)*
Box 4
Describe the likely/potential consequences of the data breach:

Box 5

Describe the measures taken/you propose to take in order to address the personal data breach:

Box 6

Date submitted to the Authority:

Box 7

If the date in box 6 is more than 72 hours after the date in box 2; explain the reasoning for a delay of more than 72 hours

(Information must not be delayed being given to the Authority because all of the information is not provided. It is acceptable under Law to provide the information in phases so as to prevent undue delays in proceedings)

Box 8

Signed:

Name:

Date:

Ensure that the Compliance and Special Projects Manager for LV Care Group is aware that this breach has occurred and that this form has been submitted to the Authority.
Email to: breach@OICJersey.org

Appendix d - Data protection training requirements for employees

All employees must receive annual training on:

- The Principles of GDPR,
- Keeping personal/special information secure,
- Disclosing client/resident personal information over the telephone,
- Handling requests from individuals for their personal information (access requests),
- The process for reporting a data breach.

(Information Commissioner's Office, 2016)

Fair processing notice for clients/residents

What we need
We hold and store data which you provide to us. This data can include your name, date of birth, address, and healthcare funding options. We also collect your health data.
Why we need it
The data we collect is collected to ensure that your care is appropriate for you. Although you have the right not to give us certain data, if you do not provide us with the data we ask for, your care may not be as appropriate as it could be. You can always add more information to the data we hold about you at a later date. To provide appropriate care, we collect data from other agencies. This may include the States of Jersey departments, your GP practice, or other care agencies you have used in the past.
What we do with it
The data which you give us is stored securely, and is accessed by our employees in accordance with your care needs. All of the data which we hold about you is processed in Jersey, Channel Islands. On occasion, we may find the need to share your data (including your health data) with other agencies. These agencies may include States of Jersey departments, your GP practice, healthcare professionals involved in your care, or others parts of the LV Care Group. We will ask you prior to making referrals and passing across this data, and will only ever pass across the necessary information required to continue your care. We do not use your data for public functions, unless there is a legal reason to do so. We will not use your data for marketing purposes.
How long we keep it for
We keep your data for the time identified by the 'Records Management Code of Practice for Health and Social Care,' by the Information Governance Alliance (2016).
Disclaimer
I confirm that I have read this notice and understand the following: - You will use the information I have provided to carry out my care in an appropriate and patient-centred way. - You may check relevant information with other sources such as States of Jersey departments, e.g. Health and Social Services Department, Social Security.

- You may also get information about me from relevant organisations, or give information about me to them to make sure that the information is accurate, prevent or detect crime, and protect public funds.
- I understand that by providing incorrect or incomplete information may impact on the care which I am given, as it may not be appropriate for my needs. In some circumstances, if I give information that is incorrect or incomplete, you may withdraw services, and take appropriate action.
- I have the right to withdraw my consent from having my data shared at any point. However, I understand that this may impact the care which I receive.
- If I am a Home Care client, I understand that whilst my care notes are stored in my home, they are my responsibility. Therefore, I understand the need to keep my care notes safe whilst they are kept in my home.

Name:

Signature: Date:

Fair processing notice for employees

What we need

We hold and store data which you provide to us. This data can include your name, date of birth, address, ITIS information, Social Security number, telephone number. We also take a copy of photographic identification.

Why we need it

We need your data in order help you carry out your terms of employment. Although you have the right not to give us certain data, if you do not provide us with the data we ask for, this may affect your employment. You can always add more information to the data we hold about you at a later date.

What we do with it

The data which you give us is stored securely, and is accessed by our employees in accordance with your employment needs. All of the personal data which we hold about you is processed in Jersey, Channel Islands. We do not use your data for public functions, unless there is a legal reason to do so. We will not use your data for marketing purposes.
In some cases, it may be relevant for us to share information with organisations such as the States of Jersey.
We use some of the information you provide us with to contact referees for references about you prior to you commencing your role. We may also need to use some of the information you provide us with for occupational health reasons such as assessment. Your information will be shared with relevant bodies so as to obtain relevant DBS checks as part of the recruitment process, if this is relevant to your role.
If relevant to your role, your personal mobile phone number is put on the duty rota, so as all of the carers can contact each other for work/client related matters.

How long we keep it for

Your employee records (including evidence of your right to work, security checks, recruitment documentation, occupational health reports, clinical training records) are retained by us for 6 years after you have left employment, or until your 75th birthday, whichever is soonest. Your statutory and mandatory training records for training undertaken with us are kept for 10 years after training has been completed.

Disclaimer

I confirm that I have read this notice and understand the following:

- You will use the information I have provided to carry out the relevant recruitment processes; this includes carrying out DBS checks and collecting references prior to my employment.
- You may also get information about me from relevant organisations, or give information about me to them to make sure that the information is accurate, prevent or detect crime, and protect public funds.
- I understand that by providing incorrect or incomplete information may impact on my employment.
- I have the right to withdraw my consent from having my data shared at any point. However, I understand that this may impact on my employment.
-

Name:

Signature: Date:

Data Protection Impact Assessment form

Data Protection Impact Assessment form
Date and time that the form was filled out
Name and contact details of manager filling out the form
Location applicable to DPIA (i.e. Lavender Villa, Cheval Roc, Rosemary Cottage or LVHC)
Will the process be running centrally (i.e. covering the whole of the LV Care Group), or locally (affecting just one subsidiary company)?
Describe the purpose of the proposed processing operation
Is there a legitimate business reason for this proposal? If so, describe this reasoning
Describe the necessity/proportionality of the processing in relation to the stated purpose in box 6

Identify potential risks to individuals (this includes employees and clients/residents)
What controls will you put in place in order to mitigate the identified risks
Are data processors involved? If yes, have they contributed to this Assessment? Describe the context of their contribution
If involving data processors, have they evidenced their GDPR documentation?
Date consulted with Compliance and Special Projects Manager
Signed: **Name:** **Date:**