



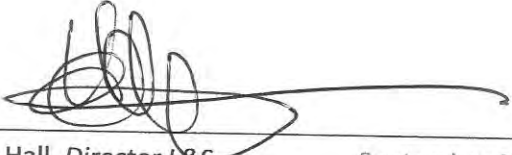
CAYMAN LAND INFO

LANDS AND SURVEY DEPARTMENT (L&S)

DATA PROTECTION POLICY

Version 1.1

Key details

TITLE:	L&S Data Protection Policy
PREPARED BY:	Angeleta Wilson-Daley, <i>Data Protection Practitioner</i>
IMPLEMENTATION:	All L&S Offices (<i>Grand Cayman and Cayman Brac</i>)
L&S APPROVAL:	 Jon Hall, <i>Director L&S</i> September 2020
EFFECTIVE DATE:	October 2020
VERSION:	1.1
RELATIONSHIP TO PREVIOUS POLICY:	Minor update to first version issued February 2020



Document Revision History

Date	Description of Change	By	Version
January 2020	First version of policy established.	A. Wilson-Daley, J. Witter, S. Williams	1.0
September 2020	Updates to hyperlinks changed during the update of Lands and Survey's website	A. Wilson-Daley	1.1

Contents

Context and overview	5
Introduction.....	5
Why this policy exists.....	5
Data Protection Law (DPL)	5
Purpose, people, risks and responsibilities	6
Policy Purpose and Scope.....	6
Data protection risks	6
Responsibilities.....	7
General staff guidelines	8
Data storage.....	9
Data use.....	10
Data accuracy.....	10
Subject access requests	11
Disclosing data for other reasons	11
Providing information.....	12
Breach Notification.....	12
Appendix.....	14
Key Links.....	14
1. Data Protection Law (2017) (DPL).....	14
2. Data Protection Regulations 2018.....	14
3. Lands and Survey Department’s Privacy Statement.....	14
4. Subject Access Request Form and Guidance Notes.....	14
5. Ombudsman’s Website	14
What are the Data Protection Principles?.....	14
What are the Individual’s Rights under the DPL?	15
DPL – Some Key Definitions	16
L&S Personal Information Inventory	17
Privacy Breach Notification Form [<i>Internal Reporting Only</i>]	19

Introduction

Lands and Survey Department (L&S) needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Department's data protection standards — and to comply with the law.

L&S is committed to ensuring the security of personal information in order to protect it from unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks.

Why this policy exists

This data protection policy ensures Lands and Survey Department:

- Complies with Data Protection Law (DPL) and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it processes individuals' data [*see definition of 'processing' in appendix*]
- Protects itself from the risks of a data breach

Data Protection Law (DPL)

The Data Protection Law 2017 describes how organisations — including Lands and Survey Department — must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Law is underpinned by eight important principles. These, concisely, say that personal data must:

1. Be processed fairly
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date

5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred to a country or territory, unless that country or territory also ensures an adequate level of protection

Purpose, people, risks and responsibilities

Policy Purpose and Scope

This policy describes the principles and practices that the Lands and Survey Department follows to protect personal information.

This policy has been developed in compliance with the requirements of Data Protection Law 2017.

This policy applies to:

- The head office - Lands and Survey Department, GAB
- Lands and Survey Department – Lands Office, Cayman Brac
- All staff and volunteers of Lands and Survey Department
- All contractors, suppliers and other people working on behalf of Lands and Survey Department.

It applies to all data that the Department holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Law 2017. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- HR records
- ...plus any other information relating to individuals

[See more detailed definitions for personal data and sensitive personal data, as well as the kinds of information that L&S may hold about you in the Appendix]

Data protection risks

This policy helps to protect L&S from some very real data security risks, including:



- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the Department uses data relating to them. [NOTE: *this cannot interfere with the statutory authority of L&S, for example: where the data is included in the public register, as we are legally required to maintain this and make it available to the public under the Registered Land Law.*]
- **Reputational damage.** For instance, the Department could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with L&S has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **Director** [**“data controller”**] is ultimately responsible for ensuring that L&S meets its legal obligations.
- The **Data Protection Practitioner**, is responsible for:
 - Keeping the Director updated about data protection responsibilities, risks and issues.
 - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
 - Arranging data protection training and advice for the people covered by this policy.
 - Handling data protection questions from staff and anyone else covered by this policy.
 - Dealing with requests from individuals to see the data L&S holds about them (also called ‘subject access requests’ – *[see definition in Appendix]*).
 - Checking and approving any contracts or agreements with third parties that may handle the Department’s sensitive data.
 - Approving any data protection statements attached to communications such as emails and letters.
 - Addressing any data protection queries from journalists or media outlets like newspapers.

- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
- The Director of Lands and Survey and/or his designated staff members in consultation with Computer Services Department (CSD), in their capacity as Government's IT Department, and the Chief Information Security Officer(CISO), are responsible for:
 - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
 - Performing regular checks and scans to ensure security hardware and software is functioning properly.
 - Evaluating any third-party services the Department is considering using to store or process data. For instance, outsourcing IT related services. This may also involve, where there are no perceived or direct conflicts of interest, the monitoring of any contracts or agreements with third parties that may handle the Department's data.

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **L&S will provide training** to all employees to help them understand their responsibilities when handling data.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the Department or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of in accordance with the Cayman Islands National Archive and Public Records Law (2015 Revision) retention and disposal schedule for the department or other relevant government policies/guidelines.
- Employees **should request help** from their line manager or the data protection practitioner if they are unsure about any aspect of data protection.



Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the data protection practitioner.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

Operational land registry records must be stored in a secured vault with direct physical access to the records limited only to L&S employees and eligible external parties accredited by L&S, such as security personnel. L&S ensures that third-party service providers such as security and cleaning personnel are supervised when they have access to the secured vault.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD/DVD or USB drive), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to **approved computing platforms**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the Department's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.

- All servers and computers containing data should be protected by **approved security software and a firewall.**

Data use

Personal data is of no value to L&S unless the department can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally.**
- Where possible, data must be **encrypted before being transferred electronically.**
- Employees **should not save copies of personal data to their own computer drives**, in particular to the “C drive” or “My Documents” folder or “Desktop”.

Data accuracy

The law requires L&S to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort L&S should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible, taking into consideration any existing laws that govern such updates.

- Data will be held in **as few places as necessary.** Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer’s details when they call.
- L&S will make it **easy for data subjects to update the information** the Department holds about them. For instance, via the Department website where possible.
- Data should be **updated as inaccuracies are discovered.** For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by L&S are entitled to:

- Ask **what information** the department holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date**.
- Be informed how the Department is **meeting its data protection obligations**.

If an individual contacts the Department requesting this information, this is called a “*subject access request*”.

Subject access requests from individuals should be made **in writing** by:

Email: dpl.lsu@gov.ky

Mail or Hand Delivery:

Data Protection Practitioner

Lands & Survey Department
Government Administrative Building
Box 120, 133 Elgin Avenue
Grand Cayman KY1-9000

The data protection practitioner can supply a standard request form, although individuals do not have to use this.

Individuals will not be charged for subject access requests, unless the request is deemed to be manifestly unfounded or excessive. The data protection practitioner will aim to provide the relevant data within 30 days.

The data protection practitioner will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

The Data Protection Law allows personal data to be disclosed to law enforcement agencies without the consent of the data subject if the personal data is being requested for:

- the prevention, detection or the investigation of a crime;
- the apprehension or prosecution of persons suspected to have committed an offence anywhere; or

- the assessment or collection of any fees or duties, or of any impositions of a similar nature in the Cayman Islands.

Under these circumstances, L&S will disclose requested data. However, the data protection practitioner will ensure the request is legitimate, seeking assistance from the Director and from the legal department where necessary.

Providing information

L&S aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the Department has a [privacy statement](#), setting out how data relating to individuals is used by the department.

[This is available on request. A version of this statement is also available on the department's [website](#).]

Breach Notification

L&S takes all data breaches seriously.

Notification of a breach should occur as soon as possible after discovering the privacy breach. **The DPL requires that all personal data breaches be reported to both the Ombudsman and the affected individuals within 5 days, unless the breach is unlikely to prejudice the rights and freedoms of the data subjects.**

Breaches can be the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorized third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Any employee who notices or becomes aware of a breach should notify their section heads in the first instance; providing as much details as possible to assist with any

investigation into such breach. Heads of sections should immediately notify the Director and the Data Protection Practitioner of the suspected breach. *[See breach form to be submitted by heads of section in Appendix.]*

The Data Protection Practitioner or the Director is responsible for notifying the Cabinet Office's Information Rights Section for guidance on the official notification to the Ombudsman and to the affected individuals.

Key Links

1. [Data Protection Law \(2017\) \(DPL\)](#)
2. [Data Protection Regulations 2018](#)
3. [Lands and Survey Department's Privacy Statement](#)
4. [Subject Access Request Form](#) and Guidance Notes
5. [Ombudsman's Website](#)

What are the Data Protection Principles?

1. FIRST PRINCIPLE

Personal data shall be processed fairly and lawfully.

2. SECOND PRINCIPLE

Personal data shall be obtained only for one or more specified lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. THIRD PRINCIPLE

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are collected or processed.

4. FOURTH PRINCIPLE

Personal data shall be accurate and, where necessary, kept up to date.

5. FIFTH PRINCIPLE

Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

6. SIXTH PRINCIPLE

Personal data shall be processed in accordance with the rights of data subjects under this Law.

7. SEVENTH PRINCIPLE

Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. EIGHTH PRINCIPLE

Personal data shall not be transferred to a country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

What are the Individual's Rights under the DPL?

Under the DPL individuals have rights in relation to their own personal data. These rights are not absolute as they may be restricted in certain specified circumstances.

Exemptions may also apply, whereby specified rights or other provisions of the DPL do not apply.

The DPL grants the following rights to individuals:

The right...

- 1. to be informed**
- 2. of access**
- 3. to rectification**
- 4. to stop/restrict processing**
- 5. to stop direct marketing**
- 6. in relation to automated decision making**
- 7. to seek compensation**
- 8. to complain**

DPL – Some Key Definitions

What is Personal Data?

“**Personal data**” means data relating to a living individual who can be identified and includes data such as –

- a) the living individual’s location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the living individual;
- b) an expression of opinion about the living individual; or
- c) any indication of the intentions of the data controller or any other person in respect of the living individual.

What is Sensitive Personal Data?

“**Sensitive personal data**” means, in relation to a data subject, personal data consisting of -

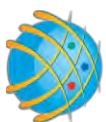
- a) the racial or ethnic origin of the data subject;
- b) the political opinions of the data subject;
- c) the data subject’s religious beliefs or other beliefs of a similar nature;
- d) whether the data subject is a member of a trade union;
- e) genetic data of the data subject;
- f) the data subject’s physical or mental health or condition;
- g) medical data;
- h) the data subject’s sex life;
- i) the data subject’s commission, or alleged commission, of an offence;
or
- j) any proceedings for any offence committed, or alleged, to have been committed, by the data subject, the disposal of any such proceedings or any sentence of a court in the Islands or elsewhere.

Who is a Data Subject and What does processing mean?

A “**data subject**” means (a) an identified living individual; or (b) a living individual who can be identified directly or indirectly by means reasonably likely to be used by the data controller or by any other person.

“**Processing**”, in relation to personal data, means obtaining, recording or holding personal data, or carrying out any operation or set of operations on personal data, including –

- a) organizing, adapting or altering the personal data; (b) retrieving, consulting or using the personal data;
- b) disclosing the personal data by transmission, dissemination or otherwise making it available; or
- c) aligning, combining, blocking, erasing or destroying the personal data



L&S Personal Information Inventory

The following is a summary of personal information under the custody or control of the Lands and Survey Department (L&S), some of which is contained in personal information banks (which are files of information that are organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual).

These files contain the names of applicants to register interest in land, customers, third parties, and L&S employees.

1. Operational Records

Land registration and survey records stored in electronic systems and paper files in vaults, staff offices and off-site storage include:

- **Land registry records** collected in relation to filings with L&S as a result of applications under legislation, including the Registered Land Law. These records contain personal information such as name and address, some also including telephone number, e-mail, occupation, unique identification numbers and others also contain personal information contained in applications or supporting documents filed with L&S in relation to interests in land (e.g. copy of passport or driving license).
- **Survey and Valuation records** collected as part of a statutory application or survey plan review in relation to carrying out statutory duties, including approving survey plans, , purchasing and selling of land and preparing Crown grants. These records contain personal information such as name, address, telephone number, e-mail, occupation, position held in a company, unique identification numbers and in some cases personal information contained in supporting documents filed in relation to survey plans and Crown grants and (historic) 'natural love and affection' submissions.

2. Administrative Records

Administrative records stored in electronic systems and paper files in vaults, staff offices and off-site storage include:

- **Land registration and survey administrative records**, including correspondence, inquiries, complaints, insurance, claims and customer records relating to land registration and survey operations. These records contain personal information such as name, address, telephone number, e-mail, occupation and unique identification numbers.
- **Customer records**, including account and inquiry information. These records contain personal information such as name, address, telephone number, e-mail, account, password and banking information.

- **Systems and security records**, including authentication, access and user login information. These records contain personal information such as name and login identifier.
- **Finance records**, including employee pay and benefit and customer payment information. These records may contain personal information such as name, date of birth, social security number, address, telephone number, e-mail, unique identification numbers, earnings, benefit entitlements, account, banking and payment information.
- **Human Resources records**, including employee pay, benefit, performance, health, educational, employment and background information. These records contain personal information such name, address, telephone number, e-mail, family status, spousal information, social security number, gender, birth date, birth place, citizenship, residency, medical, earnings, benefit entitlements, account, unique identification numbers, employment history, education, experience and employment background information.
- **Communications records**, including customer, stakeholder and employee contact, account and feedback information. These records contain personal information such as name, address, telephone number, e-mail and account information.
- **Facilities records**, including building access reports. These records contains personal information such name, and unique identification number.
- **Regulatory records**, including freedom of information access requests, complaints and policy, legal and regulatory compliance information. These records contain personal information such as name, address, telephone number, e-mail and unique identification number information and in some cases personal information relating to the details of a request, complaint or investigation.

Privacy Breach Notification Form *[Internal Reporting Only]*