



DATA MANAGEMENT POLICY

OF

THE QUEER SOCIETY

Adopted by the Board on 17/07/2025

Last updated 17/07/2025

Table of Contents

Table of Contents	2
Chapter 1. About This Policy	4
Purpose	4
Scope and Persons Affected	4
Data Management Policy Principles	4
Chapter 2. Collection and Use of Data	5
Section 1. Personal and Sensitive Information	5
Section 2. Operational Information	6
Section 3. Financial Information	7
Section 4. Low Value Records	9
Chapter 3. Data Storage	10
Section 1. Data Storage	10
Chapter 4. Data Security	12
Section 1. Data Security	12
Chapter 5. Data Breach and Non-Compliance	13
Section 1. Data Breach	13
Section 2. Levels of Breach	13

Chapter 1. About This Policy

Purpose

- (a) The purpose of this policy is to provide a framework for data management and account usage by any person with access to organisation accounts, to define the acceptable related standards in the organisation, and to promote compliance with the governance framework of The Queer Society.
- (b) Beyond legal requirements, The Queer Society recognises that there are ethical standards and community expectations regarding the management of data. It considers these standards and expectations to be impactful in operating ethically and minimising reputational risk.

Scope and Persons Affected

- (a) This is a binding policy document that applies to:
 - (i) Any individual who has or is in future given access to an account associated with The Queer Society;
 - (ii) Any individual who has or is in future given access to The Queer Society data storage through any other means.
- (b) Members are bound by this Policy at all times except when identified as being exempt by this Policy;
 - (i) For the avoidance of doubt, this Policy regarding the conduct of users applies only when they are using an organisation account which allows for the handling (inclusive of email production and receipt) of data managed and stored by The Queer Society. This does not impact the use of personal accounts for personal matters;
- (c) The Committee may grant an exemption to any part of this policy by resolution.

Data Management Policy Principles

- (a) Privacy: The Queer Society is committed to and respects the privacy of personal and sensitive information.
- (b) Transparency: The Queer Society is committed to being open and transparent in the way it operates.
- (c) Legal Compliance: The Queer Society is committed to all information being collected, used, and disclosed lawfully.
- (d) Risk Minimisation: The Queer Society acknowledges the risks associated with stored information and is committed to managing data in a manner which minimises these risks.

Chapter 2. Collection and Use of Data

Section 1. Personal and Sensitive Information

- (a) The Queer Society will only collect information if authorised to do so by law or by consent and will only collect that which is necessary for purposes which the provider can be reasonably considered aware of.
- (b) The Queer Society will always prioritise direct collection of personal and sensitive information, however, may request personal information from another authorised party;
 - (i) Information may also be obtained in investigation of non-compliance where the individual has agreed to comply with the policies of The Queer Society and information is relevant to the matter(s) under investigation;
- (c) All collection and use of data is subject to the Welfare Policy. The Data Management Policy as it relates to personal and sensitive information is to be read in conjunction with the Record Keeping and Privacy Policy outlined in the Welfare Policy.
- (d) Common methods of personal and sensitive information collection:
 - (i) When subscribing to the The Queer Society newsletter or requesting other The Queer Society related communications;
 - (ii) When applying to be a member of The Queer Society;
 - (iii) When completing The Queer Society circulated forms, including registrations for events;
 - (iv) By formal information gathering power under the Constitution and Policies (e.g. when conducting consultations related to misconduct).
- (e) The primary use of personal information is:
 - (i) To facilitate communication with individuals who have indicated they wish to receive correspondence from The Queer Society;
 - (ii) To develop a database for the purpose of demographic research. This is performed at a high level and not on an individual record level, it is de-identified and largely focuses on statistics and trends;
 - (iii) To enable appropriate judgement by selection panels in appointing representatives and other members;
 - (iv) To ensure decision making can be appropriately made with available relevant facts and circumstances presented in order to do so.
- (f) The primary use of sensitive information is:

- (i) To ensure inclusivity in the undertaking of The Queer Society. This includes, but is not limited to, being made aware of correct use of pronouns, and accessibility requests;
 - (ii) To develop a database for the purpose of demographic research. This is performed at a high level and not on an individual record level, it is de-identified and largely focuses on statistics and trends.
- (g) In general, The Queer Society will only use or disclose personal or sensitive information for the purpose for which it was collected and always in a manner which is lawful.
 - (i) There is very limited appropriate use or disclosure outside of that identified in Sections 5.7 and 5.8 of this policy. Any other usage or disclosure which has not been expressly authorised by the individual to which the information relates should be discussed with the Committee to confirm compliance with governing body regulations prior to proceeding.
- (h) All individuals who have access to the handling of personal information managed or stored by The Queer Society are made aware of their obligations to handle information in accordance with this policy;
 - (i) Where an accidental or unauthorised use or disclosure is identified, the Committee will act quickly to rectify and remedy the situation.
- (i) In the event The Queer Society becomes aware that data held is inaccurate, out of date, misleading or incorrect, proactive steps will be taken to correct the information.
- (j) Members may, in writing, request the deletion of personal and sensitive information which is to be actioned within a reasonable period of time as far as is permissible by law.

Section 2. Operational Information

- (a) The Queer Society maintains documentation of the duties of volunteers, employees and members, inclusive of the responsibility to produce and maintain operational information;
 - (i) Where there is uncertainty concerning the responsibility to produce documents, the individual or group concerned is to contact the Committee.
- (b) Examples of operational information collected by The Queer Society includes (but is not limited to):
 - (i) Meeting minutes;
 - (ii) Proposals and Reports;
 - (iii) Memorandum of Understandings and other Third Party Agreements;

- (iv) Incident and Arbitration details;
 - (v) Details of consultations performed as they relate to decision making.
- (c) Common methods of operational information collection includes (but is not limited to):
- (i) Submission to Committee or other oversight bodies;
 - (ii) Production and maintenance of minutes;
 - (iii) Performance of consultations;
 - (iv) Feedback forms;
 - (v) The Queer Society linked email accounts;
 - (vi) Reports or any other production of information stored in, or originating from, a The Queer Society linked online service;
 - (vii) By formal information gathering power under the The Queer Society's governing documents (e.g. when conducting consultations related to misconduct).
- (d) The primary use of operational information is:
- (i) To ensure decision making can be appropriately performed with relevant facts and circumstances readily accessible;
 - (ii) To comply with the record-keeping obligations as required by governing bodies and the The Queer Society's governing documents;
 - (iii) To understand and document actions, decisions, or processes undertaken in relation to The Queer Society's operations.
- (e) In general, The Queer Society will only use or disclose operational information for the purpose for which it was collected and always in a manner which is lawful.
- (f) All individuals who have access to the handling of operational information managed or stored by The Queer Society are made aware of their obligations to handle information in accordance with this policy.
- (i) Where an accidental or unauthorised use or disclosure is identified, the responsible body will act quickly to rectify and remedy the situation.
 - (ii) As far as is practicable, the responsible body will act to notify impacted parties as to the extent of the breach as quickly as is practicable.

Section 3. Financial Information

- (a) The Queer Society maintains documentation of the duties of volunteers, employees and members, inclusive of the responsibility to produce and maintain financial information.
 - (i) Where there is uncertainty concerning the responsibility to produce documents, the individual or group concerned is to contact the Treasurer.
- (b) Examples of financial information collected by The Queer Society includes (but is not limited to):
 - (i) Invoices for The Queer Society related activities;
 - (ii) Budget materials;
 - (iii) Previous financial statements;
 - (iv) Third Party and Internal Contracts;
 - (v) Forecast calculations;
 - (vi) Bank Statements;
 - (vii) Accounting Policies.
- (c) Common methods of financial information collection includes (but is not limited to):
 - (i) Submission to Committee or other oversight bodies;
 - (ii) Third Party Information and Reports (e.g. Banking, Investments);
 - (iii) Receipts and Invoices provided to The Queer Society linked accounts.
- (d) The primary use of financial information is:
 - (i) To ensure decision making can be appropriately performed with relevant facts and circumstances readily accessible;
 - (ii) To report the size of The Queer Society to ACNC to inform level of obligations;
 - (iii) To enable the preparation and sufficient review or audit of The Queer Society's financial report as required by ACNC;
 - (iv) To comply with all other record-keeping obligations as required by governing bodies and the The Queer Society Constitution.
- (e) In general, The Queer Society will only use or disclose financial information for the purpose for which it was collected and always in a manner which is lawful;

- (f) All individuals who have access to the handling of financial information managed or stored by The Queer Society are made aware of their obligations to handle information in accordance with this policy;
 - (i) Where an accidental or unauthorised use or disclosure is identified, the responsible body will act quickly to rectify and remedy the situation.
- (g) Financial decisions are likely to require quick and flexible management in order to continue compliance with related obligations and to serve the financial needs of The Queer Society;
 - (i) In the expectation of a higher frequency of change, this policy does not restrict the ability of the Treasurer to make decisions in alignment with the Constitution, Policies, and other governance requirements.

Section 4. Low Value Records

- (a) Within the categories of data identified above, exist low-value records. These records are not needed as evidence or record of the organisation's operation, financial position, or otherwise required by governing bodies.
- (b) This information is characterised by that which is short-term, facilitative, or transitory. These records, though they may have been part of a process at a specific point in time, do not in themselves have long-term value.
- (c) Examples of Low Value Records include:
 - (i) Circulation copies of relevant documents (not master documents);
 - (ii) Spam email;
 - (iii) Rough working papers or drafts not intended for further use or reference, including those which have been subsequently incorporated into final versions;
 - (iv) Duplicates.
- (d) For the avoidance of doubt, low value records do not include any information that is or *may* be required for:
 - (i) Regulatory, legal, or accountability purposes; or
 - (ii) Compliance with the The Queer Society Constitution or Policies; or
 - (iii) Information required to document a significant incident or decision; or
 - (iv) Ongoing efficiency of The Queer Society administration and operations; or
 - (v) Meeting community expectations; or

- (vi) Otherwise maintaining a complete record of decisions, reasons, significant sources of information, actions or other substantial information where this information is not contained elsewhere.

Chapter 3. Data Storage

Section 1. Data Storage

- (a) Information is stored electronically and can, in most instances, be accessed only by select The Queer Society employees and volunteers who have been provided authorisation.
- (b) Users should refrain where possible from storing information locally, or otherwise separately from a The Queer Society linked online service, for extended periods of time.
- (c) Data is to be stored for the timeframes noted below, unless appropriately reasoned otherwise:
 - (i) Personal information – for the timeframe until which the purpose for its collection has concluded;
 - (1) This includes deidentifying over time where demographic data is to be in continued use.
 - (2) This excludes information included in an incident report which is to be maintained for 7 years due to its relation to operative decision making.
 - (ii) Operational information – for a period of 7 years from the last instance of use;
 - (iii) Financial information – for a period of 7 years from the last instance of use;
 - (1) There are exceptions to this in the case of capital gains tax assets or depreciating assets in that the record will be required to be maintained for as long as the related asset is maintained and an additional five years from disposal of the asset.
 - (2) It is at the Treasurer's discretion to identify records requiring maintenance longer than the period of 7 years. It is the responsibility of the Treasurer to make the person responsible for the management of identified data aware of the requirement to continue storage.
- (d) Low Value Records – timing of deletion is at the discretion of the data manager and is not to exceed the timelines identified in Section 6. above.
 - (i) Users must consider whether the information contained can be considered a low value record in accordance with this policy;
 - (ii) Users will seek guidance prior to the deletion of data in the event of uncertainty;
- (e) All users are made aware of their obligations under this policy when they become a user, or for those existing users, upon approval of this policy by the Committee.

Ongoing monitoring is performed by the Committee who additionally provide guidance to ensure adherence to this policy.

Chapter 4. Data Security

Section 1. Data Security

- (a) Records containing sensitive information can be accessed only by those with appropriate authorisation;
 - (i) Only select users responsible for demographic research, welfare, or other relevant administrative tasks are authorised to access sensitive records;
 - (ii) Access is only considered authorised in the carrying out of the member's related duties and other access is considered misconduct being non-compliant with this policy.
- (b) On completion of a role through which an individual has been given access to a The Queer Society account capable of handling data, their access will be removed.
 - (i) No information obtained from the database maintained by The Queer Society is to be stored by the former user;
 - (ii) All relevant data maintained by the user is to be uploaded prior to the user's removal from the account and subsequently deleted from the user's personal computer or database.
- (c) All accounts used for data storage are password protected;
 - (i) All passwords must be changed at least once per year.
 - (ii) Where a user believes there may be risk of a security breach, they are to notify the Committee immediately.
- (d) All users are made aware of their obligations under this policy when they become a user, or for those existing users, upon approval of this policy by the Committee. Ongoing monitoring is performed by the Committee who additionally provide guidance to ensure adherence to this policy.

Chapter 5. Data Breach and Non-Compliance

Section 1. Data Breach

- (a) A Data Breach occurs when information is lost or subjected to unauthorised access, modification, use or disclosure or any other misuse. Authorisation in this context refers to the provisions of the Data Management Policy and that which is outlined by law.
 - (i) Whilst the process outlined in this section applies to all data breaches, in some instances legislation may impose more restrictive protocols and handling must be considered collectively with this Policy and relevant legislation.
- (b) Any employee, volunteer, or member is obligated to immediately report any suspicion of breach or misconduct under this policy.
- (c) All report submissions are to be made available to the Committee, who must assess the level of risk and determine an appropriate response.
- (d) In assessing the level of risk and appropriate response, the following questions will be considered by the Committee:
 - (i) What information does the breach involve? Is it personal or protected information?
 - (ii) What was the cause of the breach? Is there evidence or suspicion of malicious intent?
 - (iii) What is the extent of the breach? Have there been other breaches that could have a cumulative effect? Is there a risk of further exposure?
 - (iv) What are the potential harms caused by the breach?
 - (v) What is the ability of The Queer Society and the individual or group to which the information pertains to avoid or mitigate possible harm of a breach?

Section 2. Levels of Breach

- (a) Low level breaches or non-compliance include instances which have already been or can be immediately rectified with no ongoing risk. An example includes the sharing of a document with another user who did not open the document prior to access being removed.
 - (i) In the instance of low level breaches, the required action will remain at the discretion of the Committee.
 - (ii) Any action taken relating to this section is limited to that which is compliant with this policy and within their normal rights as directors.

- (b) Medium level breaches or non-compliance includes instances which are suspected to have infringed on The Queer Society's internal governance including.
 - (i) In this instance, the matter will be communicated to the Committee as soon as practicable and handled as per the Misconduct section of the Welfare Policy. In the proceedings under the Welfare Policy, the following details must be recorded:
 - (1) A description of the breach or suspected breach;
 - (2) Action taken by the Committee or others to address the breach or suspected breach;
 - (3) Outcome of the action taken;
 - (4) Confirmation that no further action is required and the matter does not reflect a high level breach or misconduct.
- (c) High level breaches or non-compliance includes instances for which there is evidence of an actual or reasonably expected breach of The Queer Society's legal obligations or responsibilities to governing bodies or it is otherwise determined that a serious breach or instance of non-compliance has occurred at the discretion of the Committee.
 - (i) Direct engagement of the personnel involved is subject to the Welfare Policy, however, legal handling and proceedings remains at the discretion of and the responsibility of the responsible persons.
 - (ii) Where it is identified that third parties must be notified, this is to be done directly and as soon as reasonably possible.
 - (1) In general, notification should be direct to affected individuals.
 - (2) Indirect notification, for example by website or social media, should only occur where direct notification could cause harm, is cost prohibitive or the individual's contact information is unknown.
 - (3) Third parties include, but are not limited to:
 - i. Individuals or groups to which the information pertains.
 - ii. The ACNC or other regulatory body;
 - iii. Financial Institutions;
 - iv. The Police;

- (iii) In the instance of all levels, where immediate action is identified as readily available to contain or resolve the breach, the relevant Committee will not be prevented from taking this action to address the breach or misconduct.
- (iv) Immediate action taken by the Committee to address misconduct under this policy includes (but is not limited to):
 - (1) The changing of access rights to that which is appropriate.
 - (2) The issuance of communications not to open or distribute information shared.
 - (3) The issuance of instructions to users to contain or resolve the breach.
 - (4) The resetting or requested resetting of passwords or other details for accounts inappropriately accessed.
 - (5) The reasonable querying of users for further information required to assess the risk level.