POLICY AND PROCEDURE
Privacy and information management

Contents

1. Introduction

Lighthouse Church recognises the need to collect, store and use personal information in an effective and responsible way in line with requirements, and individual and community expectations. This document provides guidance for Lighthouse staff, leaders, and ministry workers in relation to privacy and information management including cybersecurity.

2. Definitions

Personal information is information about an identified individual, or an individual who is reasonably identifiable.

Sensitive information is a subset of personal information subject to tighter privacy regulation such as health information, religious beliefs, and sexual orientation.

Cybersecurity is defined as any action taken to protect electronic information from unauthorised access.

Information asset is defined as any data, document, or other information-based resource that is owned, managed, or maintained by an organisation including physical and digital information, such as documents, images, videos, audio files, databases, and websites.

Data breach is any situation where personal information is accessed or disclosed without authorisation or is lost.

3. References

Legislation

Privacy legislation[1] is designed to protect an individual's personal information. The 1998 Act includes thirteen principles that set out the 'standards, rights and obligations for handling, holding, accessing and correcting personal information'. For more detailed information:

- see Appendix 1 for an overview of principles relevant to LIghthouse Church
- the Office of the Australian Information Commissioner (OAIC) http://www.oaic.gov.au/privacy/about-privacy

Lighthouse Church as a small not-for-profit organisation with an annual turnover of less than $3 million is not subject to the privacy principles, or to the mandatory Notifiable Data Breaches (MNDB) scheme requiring notification of the Privacy Commissioner and affected individuals in the event of an eligible data breach of their personal information. However, these policies and procedures have been developed in line with the privacy principles and cybersecurity toolkit recognising they outline good practice for all organisations.

Australian Charities and Not for Profits Commission (ACNC)

The ACNC requires registered organisations to comply with *ACNC Governance Standards* including Standard 3 - Compliance with Australian law, and Standard 5 - Duties of Responsible People which include setting policies and processes for managing people's information and data including cyber security.

The ACNC webpage *Managing people's information and data* provides helpful information including the following statement: 'Community members have clear expectations about the way a charity manages information and data. People are increasingly aware of the importance of privacy and information and data protection, and simply complying with all the base requirements of the law may not necessarily meet reasonable community expectations of responsible, honest and ethical practice. Aspiring to best practice should be the aim … It is necessary to ensure there are good policies and processes for information and data management'.

[1] Privacy Act 1988 (Cth.), Privacy Regulation 2013 (Cth.), and Privacy and Personal Information Protection Act 1998 (NSW)

The ACNC also provides a Cyber security governance toolkit which includes the following resources:

- Cyber security checklist
- Data breach response plan
- Information Asset register.

Lighthouse Church Constitution

Our church Constitution outline 'rules' that describe how our Incorporated Association 'is governed' to meet requirements under the Associations Incorporation Act 2009 (NSW). The Constitution outlines administrative aspects such as who can be an 'office bearer', membership, conducting meetings, and handling disputes.

4. Privacy policy

Lighthouse Church is committed to ensuring that personal information provided and maintained by Lighthouse Church is managed carefully and respectfully in accordance with the *Australian Privacy Principles.*

Information we collect

We collect personal information from you when you complete:

- welcome cards in church
- membership application and ministry information forms
- activity registration forms
- attendance records
- employee records
- feedback forms
- incident report forms
- safe ministry (child protection) checks and training records.

We only collect information that is necessary and relevant to your involvement in Lighthouse Church.

How your information is used

Personal information provided by you will only be used for the purpose of your participation in Lighthouse Church activities and events. Your personal information will not be disclosed to any other entity outside church unless:

- it relates directly to the functions and activities of church, and your consent has been obtained or is implied by your initiation of, or involvement in, a particular process or activity e.g. safe ministry training provider
- it is required to provide appropriate care in an emergency situation e.g. to a medical provider
- it is required by law e.g. reporting reportable conduct to the appropriate government authority.

How your information is stored

Personal information collected by Lighthouse Church is stored and accessed through Elavanto – our web-based online church community database. The database has appropriate security settings to limit access of information by position/role to those who have a need to access information.

Members of Lighthouse Church who have completed an information consent form are given a personal login allowing access to Elvanto. You can use your personal login at any time to access, review and change the privacy settings on your personal profile.

Some information is stored in Google Drive with appropriate security measures that limit access to those who have a reasonable need to access the information in line with their role in church. In some cases, information may be stored on Lighthouse Church local computer systems with appropriate password security.

We prefer to keep operational records electronically on systems with passwords to restrict access. If hard copy forms are retained, the forms will be stored in lockable filing cabinets in the office of staff, the Secretary or Treasurer.

The time period we keep personal information depends on the purpose for which it was collected. Some records may be disposed of within one year. Other records will be retained for seven years in accordance with legislative obligations. Some information needs to be retained for extended periods (no less than 50 years) in accordance with safeguarding and insurance requirements and recommendations.

We dispose of personal information carefully. Any paper records will be shredded prior to disposal. Electronic information will be deleted, and redundant system hard drives will be wiped or destroyed prior to disposal.

Updating your information

We recognise the importance of ensuring your information is current, accurate and relevant. If you are a member of Lighthouse Church, you will have a login to Elvanto so you can view and update your information at any time.

You can request access to your personal information by submitting a request to admin@lighthouse.net.au We will review and respond to your request within 14 days.

Protecting your information

We have privacy and information management procedures to ensure your personal information is protected from misuse, unauthorised access, alteration, disclosure or loss. Our procedures include the following:

- practices and expectations of staff and administration relating to privacy and information management
- practices and expectations of members in relation to privacy
- a response plan relating to a breach of privacy or information security.

5. Cybersecurity policy

We are committed to ensuring that personal information provided is maintained carefully and respectfully. This includes taking appropriate action outlined below to protect electronic information from unauthorised access.

Identify and assess the risks

Our Information Asset Register[2] forms the basis of our cyber security risk assessment approach. The register assists us to identify and prioritise risks and develop an annual action plan that is incorporated into our overarching Safe Ministry Action Plan. This is one element of our broader annual risk assessment and planning.

[2] Internal file saved in Google Drive policies and procedures folder: Privacy and Information Management.

Prevent incidents and manage risks

As a key component of protecting personal information and our information assets we use third party online services with industry standard risk management controls.

We have volunteers within our organisation with IT skills and experience who provide assistance, however we do not have dedicated IT support and sometimes we may have to engage assistance from a relevant third party. We identify opportunities to address cyber security risks, and include action where possible in our Safe Ministry Action Plan.

Take action and respond effectively when concerns, suspicions or complaints arise

Lighthouse Church's Complaints and Feedback form is available on our website and can be used to advise of any concerns or complaints relating to privacy and information management.

We have a response plan developed in line with the Australian Information Commissioner's guidance to guide prompt and effective action to address any concerns or issues relating to information management complaints, breaches, or cyber security incidents.

6. Privacy and information management procedures

6.1 Collection of personal information

Personal information is only used for the purposes of, and use by, Lighthouse Church. Newcomers are invited to record the information they are comfortable providing on the welcome card. Contact details are entered into Elvanto for the purpose of following up where appropriate.

People who wish to become a member of Lighthouse Church complete online membership and information consent forms as part of the membership process. This information is also entered into Elvanto.

Other information that may be collected and stored includes incident report forms, working with children clearances and evidence of completion of safe ministry training, permission forms, limited banking information provided by members for the purpose of giving to church (generally this is only viewed by the Treasurer).

6.2 Lighthouse Church online database

Our online database (Elvanto) is the preferred method of locating and utilising the contact details of other members. This ensures contact information is up to date, and privacy features of the program assist in ensuring people's contact information is protected and used appropriately and wisely.

Elvanto allows varying degrees of access privileges to be set according to authorised/allocated roles in church:

- staff and system administrators can view all information on the Hub
- growth group and ministry leaders can view the details of members in the groups they lead
- formal members who sign an information consent form are given a personal login to access the Hub as a basic user[3]
- privacy settings for non-members and children/youth are not listed/viewable by basic users.

[3] A login as an unlisted, limited access user may be given to a person attending Lighthouse Church regularly who is in the process of becoming a member, or a person aged 16-17 years attending either attending Lighthouse Youth or involved in a ministry team.

Members can change their own personal information, privacy and communication settings at any time. If members leave Lighthouse Church their login is made inactive as part of the membership deactivation process, and their personal information is archived.

In relation to email correspondence sent to all formal members:
- only staff and system administrators are authorised/able to do this
- these emails will be sent via Elvanto
- content must be relevant to the majority of formal members and relate to church functions and activities
- will not be used to advise of changes to member contact details, raise money, circulate personal prayer requests, or to convey or promote personal opinions of individuals in church.

6.3 Church contact lists

This list can be generated via Elvanto as required to organise church events, or on request for members who do not have regular access to a computer. Access to the contact details of other members is a privilege. Please consider the following:
- not everyone enjoys or is open to receiving a lot of email communication
- unsolicited 'broadcast' emails to all members or large groups is considered misuse of contact information
- there is no valid reason to email large groups without authorisation eg event organisers
- the purpose of the database is to help members connect and care for each other in church – using the contact information for reasons that do not fit with this purpose is considered a misuse of this information
- if you have any doubt about whether your use of member's personal information would be appropriate seek input from your growth group or ministry leader or email admin@lighthouse.net.au

If there is a time where contact information is considered to be misused, staff or a leader will address the matter directly with the person to explain the situation and ensure it does not happen again. If there are any further concerns, access to Elvanto will be suspended as a necessary step in ensuring personal information provided and maintained by Lighthouse Church is managed carefully and respectfully.

6.4 Church website

Our website address is www.lighthouse.net.au There is the option to make some areas of the website accessible only to members who have completed an information consent form.

6.5 Photographs

Guidelines for **taking** photos

When taking photographs at Lighthouse Church events for church purposes the following guidelines should be considered:
- ask permission - if someone declines or expresses discomfort avoid taking their photograph
- photographs of children or youth should focus on the activity and the group, rather than an individual
- avoid taking photos of people that may cause embarrassment or discomfort
- avoid using photos of people who have left church for promotional purposes
- if in doubt don't take the photo.

Guidelines for **using** photos

The Privacy Act 1988 requires that photos which allow the identity of a person to be determined (eg publishing their name, or photographing a child in their school uniform) should only be published after obtaining the consent of the person, or of a child's parent or guardian.

Where possible use photos of formal members as they are given the opportunity to 'opt out' of photos used to promote Lighthouse Church on the information consent form completed as part of the membership process. A few formal members have not provided consent to use photographs of them in promotional material for Lighthouse Church. This information is recorded in our online database (Elvanto). Anyone involved in producing promotional material for Lighthouse Church should ensure photos selected for use do not include people on this list.

For children and youth, general permission to have photos taken is gained on the information consent form (for children of formal members) and on registration forms. It is preferable that members are asked about using a specific photo for external promotional purposes, particularly if the photo focuses on them as an individual or is of a child or young person.

Photos of visitors or non-members should not be used for promotional purposes or in public media without permission (preferable written). In the case of youth, permission should be sought from both parents and the young person themselves. See 'Facebook' below for information regarding use of photos on Facebook.

In NSW, it is an offence to publish identifiable material of a child who is involved in the Children's Court or non-court child protection proceedings[4]. Once a matter has been finalised, permission may be sought from the relevant parent or carer to publish photos providing no identifiable information is published (name, address, care status, history) and no identifiable information is included in the photo (ie location, school etc). However, generally it is recommended that those involved in publishing photos for Lighthouse Church avoid using images of children or youth who are or have been in out-of-home care or involved in child protection, family court or criminal proceedings.

Members, visitors and members of the public can advise of concerns about use of any image relevant to them or their family and/or can withdraw their consent for use of photographs relevant to them or their family used in promoting Lighthouse Church by email: admin@lighthouse.net.au

6.6 Prayer

Members who have completed an information consent form can choose to be involved in making and receiving prayer requests via email. Members can opt out by ticking the relevant box on the information consent form or by emailing admin@lighthouse.net.au Prayer requests should generally be limited to requests for Lighthouse Church attendees and their immediate family. Prayer requests relating to friends or other family can be raised via growth groups.

Prayer in church may include prayer for the needs of specific individuals. It is good practice to check with the person they are comfortable with this beforehand.

[4] NSW Children and Young Persons Act 1998 section 105

6.7 Facebook social networking site

Church uses Facebook pages and groups that people can opt into if they choose. Public Facebook pages may be used for youth activities for communication purposes. No photos are to be posted on Facebook unless parents have given written consent (eg via a Lighthouse Youth general permission form). Photos posted on facebook will be classed as 'advertising' and the security settings of any facebook page will be set to restrict non-administrators from posting photos.

6.8 Request for access to personal information

Australian privacy law provides people with a general right to access their personal information held by Lighthouse Church on request. This does not include other information such as commercial information.

People wanting to access their personal information can email admin@lighthouse.net.au The following information should be provided: name, contact details, a description of the personal information the person wants to access, how they would like to receive the information (eg email, post, view online).

The request will be reviewed and a response provided (usually by reply email) within 14 days. Sometimes, in line with the Privacy Principle Guidelines (Chapter 11), there may be reasons for not providing access. We will advise in writing if this is the case and let you know what you can do about it (e.g. other options and/or how to make a complaint).

6.9 Frequently asked questions

The following frequently asked questions relevant to Lighthouse Church were developed with reference to information provided on the Office of the Australian Information Commissioner's website:

a. *Can the names of people be mentioned in public prayer?*

   Yes, as long as it is within the person's reasonable expectations of what will happen with their personal information. However, It is good practice to check with the person first - especially in relation to sensitive health or personal difficulties.

b. *What do I need to think about if I want to put photos on the web?*

   When taking photos take reasonable steps to explain who you are and what you are taking their picture for. It is good practice to seek a person's express consent to use their image on the web or in written material, particularly when using images of children. If you then use the picture for something that you didn't tell the individual about, you will need the individual's consent, unless they would reasonably expect you to use their photo for this other purpose.

c. *Can we build up personal profiles of people as part of developing a relationship with them (for example by recording information they provide about their interests)?*

   Yes this is acceptable, however there are some restrictions:
   - you cannot use unfair means to collect the information eg deception, surveillance
   - if the information is then to be used for some other purpose, it can only be used if the person would reasonably expect that to happen or if they have consented
   - if collecting sensitive information, you must have the consent of the individual.

d. *Do people need to consent in writing to the use of their personal information?*

   Sometimes it may not be obvious whether someone has consented to all the uses of personal information that the organisation has in mind. The *Privacy Act* states that consent can be 'express' or 'implied'.

7. Cyber security procedures

As a small not-for-profit organisation with a high proportion of volunteers using their own devices we are at high risk of a cybersecurity incident. We mitigate this risk by using reputable third party services and products with strong controls. In addition, we have used the Australian Government's essential 8 mitigation strategies (see Appendix 2) to inform procedures and practices outlined below.

Provision and acceptable use of IT resources

On commencement of employment, Lighthouse staff at a minimum will require a suitable laptop, keyboard, mouse, monitor and mobile phone. Necessary software licences will be provided as required, and staff will be allocated a Lighthouse email address for work use. This enables Lighthouse to restrict use of IT resources to acceptable uses only and to specify offboarding procedures when employment ends. See *LC02 Recruitment and staff* for more information about these important aspects of our cybersecurity controls.

IT security requirements

Lighthouse Church does not have dedicated IT support. Staff (and ideally volunteers) performing work for Lighthouse Church have a role in reducing the risk of cyber security incidents and loss or compromise of Lighthouse information assets. For this reason, staff (and others) are asked to utilise the checklist below to inform and implement prevention strategies outlined below on personal devices used to perform work for Lighthouse Church.

What I need to do		Please circle	Notes
1. Ensure other people do not use your device or know your passwords	Prevent unauthorised access	Yes No	
2. Use a complex password or biometrics to access your device		Yes No	
3. Set your device to auto-lock after an appropriate period of inactivity		Yes No	
4. Remove services and applications no longer supported/updated by vendors	Vendors release updates to address newly identified vulnerabilities and defend against digital break-ins.	Yes No	
5. Turn on auto updates for applications (eg Microsoft Office) and operating systems (eg Windows)		Yes No	
6. Apply updates as soon as practical after a notification has been received		Yes No	
7. Ensure reputable third party antivirus is installed and and up to date on PCs	Reduce cybersecurity risk	Yes No	
8. Use passwords for online services that are at least 10 characters long, a mix of non-consecutive letters and cases,		Yes No	

numbers and symbols, and are not used for any other service			
9. Store passwords in a reputable password manager such as Bit Warden (not in web browsers)		Yes No	
10. Turn on multi-factor authentication for online services (where available)		Yes No	
11. Do not open links or attachments in emails from senders you don't know or didn't expect to receive	Common cybersecurity threat	Yes No	
12. Verify unexpected or unusual requests (eg provide account details, change direct deposits) before taking action		Yes No	
13. Preferred services and applications listed in Lighthouse's Information Asset Register and applications are used where possible.	Reputable providers and products	Yes No	
14. Only install software that is reputable and after careful consideration and research of security risks	Software can transmit malware that can cause operational issues and data loss	Yes No	
15. Store Lighthouse information in the approved file management (currently Google Drive) – not on personal devices.	Availability of information, and prevention of loss	Yes No	
16. Do not use external hard drives or USB drives to store or transfer sensitive data.	Can be lost or stolen and can fail	Yes No	

Staff should raise questions relating to the above security requirements through usual reporting channels.

Privacy or data breach response plan

The Office of the Australian Information Commissioner's Data breach preparation and response forms the basis of our response plan where unauthorised access or disclosure of information that is likely to result in 'serious harm to the individual'.

The guide and recommended approach acknowledges 'there is no single way of responding to a data breach' and 'each breach will need to be dealt with on a case by case basis undertaking an assessment of the risks involved, and using that risk assessment as the basis for deciding what actions to take in the circumstances'.

The following steps are outlined to provide guidance in responding to a breach or suspected breach:

a. Contain the breach and assess the effect including risks

- Take immediate action to limit or contain the breach. This may include changing passwords, disabling user accounts, or shutting down relevant PCs.
- Any suspected breaches should be reported to the relevant staff member who is responsible for contacting the assigned Lighthouse Administrator of the relevant service (refer to the xxx Register) to assess effect/risks:
  - how significant was the information
  - how many people are affected
  - how could the information be used
  - what will or could the impact be? financial, reputational, for who?
  - have we been able to or can we prevent the likely risk of serious harm with remedial action.

b. Take action to mitigate risks

The Lighthouse Administrator of the relevant service will take steps to address the issue and/or advise on action to be taken e.g. lodging a service request, or seeking professional advice. Staff will determine the need to notify individuals who may be affected and who is best placed to notify. Where necessary, this will be addressed as soon as possible to enable individuals to take action to limit the effect or risk.

c. Take steps to prevent future breaches

As soon as possible, staff and the Lighthouse Administrator will review the breach and response including:

- understanding how the breach occurred
- identifying opportunities to strengthen policies, procedures and practices to prevent another breach occurring
- updating systems or technology if the breach was due to a technical vulnerability
- the need for training for staff and other leaders
- the addition of any ongoing actions to the annual safe ministry plan.

8. Training and review

Staff and other 'responsible people', leaders, and our IT team are aware of this policy and procedure and the need to conduct work in line with these requirements. This document is available on our website.

This document is reviewed at least annually on completion of our annual review and risk assessment update at the end of each year, or as the need arises throughout the year.

9. Questions or concerns

If you have any questions or concerns relating to privacy or information management at Lighthouse Church please email admin@lighthouse.net.au

10 . Related policies, procedures and tools

LC02 Recruitment and staff
Lighthouse Church Information Asset Register

Appendix 1 - Overview of privacy legislation (principles)

Privacy legislation[5] is designed to protect an individual's personal information. The *Act* includes thirteen principles that set out 'standards, rights and obligations for the handling, holding, accessing and correction of personal information'. The privacy principles outline good practice to guide the practice of all organisations. The principles are summarised below:

Open and transparent management of personal information (Principle 1)

- will have practices, procedures and systems to enable the entity to deal with inquiries or complaints
- have a clearly expressed and current privacy and information management policy
- outline what information we collect and hold, why and how, and how someone can access or correct it.

Collecting of personal information (Principles 2-5)

Includes:

- Principle 2 — anonymity and pseudonymity
- Principle 3 — collection of solicited personal information
- Principle 4 — unsolicited personal information
- Principle 5 — notification of collection.

In summary:

- Information collected should be reasonably necessary for, or directly related to, the organisation's functions or activities eg do we need to collect Medicare numbers when children won't be refused treatment and we can typically get this information from parents if/when needed?
- Sensitive information should not be collected without explicit consent.
- Information should be collected directly from the person where reasonable and practicable.
- There should be the option for people to provide information anonymously where practical e.g. surveys.

Managing personal information (Principles 6-11)

Includes:

- Principle 6 Use or disclosure - personal information will be used only for the primary purpose and related purposes as reasonably expected, consent must be obtained to use for any other purpose, need actual (not implied) informed consent (including implications of consenting or not) to disclosure sensitive information
- Principle 7 Direct marketing - personal information will not be used for 'direct marketing' unless the organisation collected the information from the person, the person would reasonably expect the organisation to use/disclose information for that purpose, and a way is provided for a to easily request not to receive direct marketing communications from the organisation.
- Principle 8 — cross-border disclosure of personal information not permitted
- Principle 9 — do not use a person's government related identifier as our identifier of the person.

Integrity of personal information

Includes:

- Principle 10 Quality of personal information - take reasonable steps to ensure personal information collected, used or disclosed is accurate, up-to-date, complete and relevant, especially information that reflects badly on a person or cause harm or loss

[5] Privacy Act 1988 and Privacy Regulation 2013.

- Principle 11 Security of personal information - take reasonable steps to protect information from misuse, interference, loss, unauthorised access, modification or disclosure, and in disposing of personal information (destroy or de-identify).

Access and correction of personal information

Includes:

- Principle 12 Access to personal information - must, on request by the person, provide access to personal information held within a reasonable period (exemptions apply)
- Principle 13 Correction of personal information - take reasonable steps to ensure personal information held is accurate, up to date, complete, relevant and not misleading, personal information should be corrected if the organisation identifies the need, or the person requests correction.

Appendix 2 - Essential eight cybersecurity mitigation strategies

The Australian Government developed the 'essential eight' mitigation strategies to help organisations protect against cyber threats. As a small not-for-profit organisation we are currently unable to implement all recommended strategies. Red text below is our analysis of our current ability to implement the recommended strategies. However, this information informed our cybersecurity policies and procedures and safe ministry plan which includes activities to improve cybersecurity.

Patch applications and operating systems

An automated method of asset discovery is used at least fortnightly to detect assets for vulnerability scanning activities. Not feasible as our devices are not in a central location.

A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. Third party product. We could install it but someone has to manage this and we don't have a dedicated IT person.

A vulnerability scanner is used at least:

- daily to identify missing patches or updates for vulnerabilities in online services and operating systems of internet-facing servers and internet-facing network devices. Reliant on third party controls.
- weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. No dedicated IT person to manage this.
- fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices. No dedicated IT person to manage this.

Patches, updates or other vendor mitigations for vulnerabilities in:

- online services and operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release for critical vulnerabilities and 2 two weeks when non-critical. Reliant on third party controls.
- office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release. Addressed by action to update applications.
- in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release. Reliant on third party controls.

Online services that are no longer supported by vendors are removed. We only use supported services.

Operated systems no longer supported by vendors are updated or the PC is replaced. Action taken for Lighthouse Church devices e.g. Windows 10 not supported from Nov 2025, will need to upgrade to Windows 11 or be replaced.

Office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed. Staff to action when notifications are received.

Multi-factor authentication

Multi-factor authentication (MFA) is used to authenticate users to:

- their organisation's online services that process, store or communicate their organisation's sensitive data. We only use third party online services.
- third-party online services that process, store or communicate their organisation's sensitive data. Yes, see register. Any new services will be set up to have MFA turned on.
- third-party online services that process, store or communicate their organisation's non-sensitive data where available [ie we can use a service that doesn't have MFA but if it has it we will turn it on]. Yes, see register.
- their organisation's online customer services that process, store or communicate sensitive customer data. Yes, wherever we can. Only organisational staff and members use services.
- third-party online customer services that process, store or communicate sensitive customer data.

MFA is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.

Restrict administrative privileges

Requests for privileged access to systems, applications and data repositories are validated when first requested. Yes, administrators approve in line with policy and procedures.

Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access [Do administrators have a separate account for administrator or are they doing this from their everyday account]. Yes for Office 365 applications. Recommend to Administrators for other applications that we transition to this in our 2025 plan, particularly for our main file storage and management service (Google Drive).

Privileged users use separate privileged and unprivileged operating environments.

Privileged user accounts:

- are prevented from accessing the internet, email and web services (excluding those explicitly authorised to access online services)
- explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.
- cannot logon to unprivileged operating environments (excluding local administrator accounts).

Privileged user account will be used for administrator purposes only.

Unprivileged user accounts cannot logon to privileged operating environments.

Application control

Application control [systems to prevent unauthorised applications or programs from running]:

- is implemented on workstations
- is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.
- restricts execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to organisation-approved set.

Not feasible. Everyone would have to log into a domain or third party service that allows for those restrictions, and we don't have dedicated IT support.

Restrict Microsoft Office macros

Microsoft Office macros:

- are disabled for users that do not have a demonstrated business requirement.
- in files originating from the internet are blocked
- security settings cannot be changed by users.

Anti-virus should be provided and active on all Lighthouse devices. Others actions not currently feasible as we don't have dedicated IT support. Included in 2025 plan.

User application hardening [limiting what application can do]

Internet Explorer 11 is disabled or removed [no longer supported]. Web browsers do not process Java from the internet, process web advertisements from the internet, and web browser security settings cannot be changed by users.
Not feasible. Everyone would have to log into a domain or third-party service that allows for those restrictions.

Regular backups

Our business continuity strategy is to reinstall or buy new device as all our information stored on the web.

Backups of data, applications and settings are:

- performed and retained in accordance with business criticality and business continuity requirements
- retained in a secure and resilient manner
- synchronised to enable restoration to a common point in time.

Data back-up is managed via third party controls – see register. Device back up (application and settings) are not relied upon for business continuity.

Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises. Not relevant. We don't have back-ups.

Unprivileged user accounts cannot access backups belonging to other user accounts and are prevented from modifying and deleting backups. Addressed by recommendation to have separate administrator and everyday accounts.