St Vincent de Paul Society
NSW
good works

Acceptable Use of Technology Policy

Document number: PO2022-009

Approval

Policy owner	Chief Financial Officer		
Approved by	Executive Leadership Team State Council		
Date approved	29.09.2021 19.02.2022	Review date	19.02.2024

Purpose

1. The St Vincent de Paul Society NSW ('the Society') relies on the use of technology such as Internet and digital media to support the Society's business operations and services. The Society's personnel, supporters, and the people we assist all rely on the Society to keep their information secure.
2. The Society also has confidential information and requires all users to adhere to this policy regarding the acceptable use of technology.
3. The overriding purpose of the policy is to:
   - protect the integrity of the Society's data
   - ensure effective use of the Society's resources
   - set the Society's expectations for all users of information services technology provided by the Society or used to perform the Society's work.

Scope

4. This policy applies to all Information Services which includes, but is not limited to:
   - hardware - personal computers, laptops, tablets, smart phones, servers
   - software - business applications (such as Great Plains, Customer Relationship Management systems), access to the Society network (including email, calendar, contacts and other related functions), other internal network resources and internet access.
   - information stored on Society systems that is kept or used on-site or off-site, whether before, during or after work hours and/or provided by or at the expense of the Society.
5. This policy applies to all Society Personnel that are provided with an electronic identity to access the Society's Information Services. For the purpose of this policy the term 'user' includes all of the above.
6. This policy does not apply to Social Media use. Social media use is covered by:
   - NSW Social Media Policy

Related policies and procedures

7. Related policies and procedures include:
   - Code of Conduct
   - Information Security Policy
   - Privacy Policy
   - Records Management Policy
   - St Vincent de Paul Social Media Policy approved by National Council
   - St Vincent de Paul Society Social Media Handbook approved by National Council
   - NSW Social Media Policy

Policy principles

8. The Society grants users access to and/or supplies technology when it is required to perform the duties of their role. All users must agree to continuously adhere to the provisions of this policy and related procedures.

9. All users must provide signed acknowledgement of their acceptance of the Acceptable Use of Technology Policy.

10. The Society is committed to ensuring that all technology is used ethically and legally. The Society will co-operate with State and Commonwealth law enforcement authorities in any investigations involving suspected illegal unacceptable use (e.g. intellectual property/privacy/copyright issues).

11. Users may be subject to disciplinary action if they are found to have contravened any part of the Acceptable Use of Technology Policy which may include internal disciplinary processes, disconnection from the Society's technology systems, dismissal or legal action including prosecution for committing a criminal offence.

Email and Internet Usage

12. Users must have a secure email/system user-name and password to protect the Society's technology.

13. The internet is inherently insecure. When communicating personal, sensitive information or health information users must use secure channels provided by Society's Information Services (e.g. using https enabled websites, password-protecting documents when sharing over email).

14. Use of public Wi-Fi hotspots should be considered a last-resort. Users may only use a public hotspot if:

    - the hotspot requires use of a venue supplied, secure password
    - and the service connection is via a secured browser.

    Users should contact the Technology Services Service desk if they are unsure or require more information regarding the use of Wi-Fi hotspots.

15. The Society is responsible for material that is sent or displayed in the course of, or arising out, of users' employment with the Society.

16. Users bear responsibility for any material that they access, send, display or store on the Society's Information Services (e.g. email, web browsing, and application usage) which is not arising out of their employment with the Society.

17. If users are unsure of the nature of an attachment, internet link, file, or the identity of the sender, they should not open the file/link/or attachment until they are able to confirm its legitimacy. If they are not able to confirm legitimacy themselves, they must contact the Technology Services Service Desk for advice.

18. Users must send e-mails on a 'need to know' basis. When using the "reply all" email function, users must be confident that all recipients need to receive the information.

19. The Society’s technology should only be used to access the following types of e-mail accounts:

    - Society e-mail account i.e. vinnies.org.au
    - Google (Gmail) or Microsoft (Hotmail or Outlook.com) provided account
    - any other account which is whitelisted by technology services.

20. The Society may require the application of additional security controls to personal devices/s used to access the Society’s information Services.

21. Users must not:

    - use any system other than the Society’s approved email services for conducting Society business
    - use the Society’s information services for personal for-profit activities, (for example, personal business transactions) or unauthorised personal not-for-profit activities such as fundraising activities that are unrelated to the Society
    - create or send e-mail or other electronic communications under another person’s name or otherwise obscure the identity of the originator, except where the individual has explicitly been given delegated authority within the email system to send emails on behalf of another person
    - create, send or forward:
        - electronic chain letters, unsolicited broadcast emails (“Spam”), obscene, abusive, fraudulent, threatening or repetitive messages
        - jokes, video clips, images, text, or other content which contain material or words that negatively reflect on a particular race, gender, religion, colour, ethnicity, disability, sexual preference, marital status, or status as a parent/guardian
        - content that reflects negatively on the Society, its personnel, or professes a different position to the Society’s official position to external parties (except in the case of a whistleblower complaint or engagement with a trade union)
        - content which breaches the duty of confidentiality to the Society or people we assist
        - content that contains any promise or undertaking on behalf of the Society unless the content has been approved and/or is in keeping with the users’ delegated authority
        - content which is inappropriate or unlawful, including being contrary to the Spam Act 2003 (Cth) or the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs) under that Act. For more information, see the Society Privacy Policy
    - change the security settings of their e-mail software and Internet browser on a corporate device (e.g. laptop, desktop or mobile phone)
    - download obscene digital material or pornography
    - attempt to compromise the security of a computer
    - send emails containing passwords in clear text

- automatically forward their Society e-mail to an external e-mail address, unless authorised to do so by their line manager in conjunction with the Information Security Officer
- use the Society's information services in a way that infringes the copyright or moral rights of the Society or other people.

22. The Society will:

- capture and review all emails transmitted using a Society computer system
- use or disclose the captured emails only for risk management purposes, or for purposes which are allowed by the Workplace Surveillance Act 2005 (NSW)
- prevent delivery of non-compliant emails (e.g. emails of excessive size).

23. The Society will not prevent the delivery of an email, or access to a website in relation industrial relations where the website is owned by:

- the Fair Work Ombudsman https://www.fairwork.gov.au/
- a Trade Union registered in Australia.

24. Users must only participate in Internet based conferences, newsgroups, bulletin boards, email list servers and other collaborative electronic discussion forums if:

- they are relevant to the Society's business or the users' area of expertise, and
- the user is expressly authorised to do so by their line manager. When using these collaborative electronic discussion forum users must not give the impression that they are representing the Society or making a statement on behalf of the Society unless authorised to do so.

Limited incidental personal usage

25. While the Society Information Services such as email and Internet access, are provided for business related services, limited incidental personal use is allowed as long as such use:

- is lawful and compliant with the Society's policies and external legislation
- does not negatively impact on the users' work performance
- is infrequent
- does not hinder the work of others or interfere with the normal operations of the network
- does not damage the reputation or operations of the Society
- does not impose unreasonable or excessive additional costs on the Society
- does not include audio or video streaming such as YouTube or Spotify.

Copyright and intellectual property usage

26. Files in each user account, email and other data on the Society's Information Services are the property of the Society. The Society acknowledges that in certain circumstances the Australian Privacy Principles may apply to employees' e-mails but only in so far as they contain personal information that is not employee records or related to employee records.

27. Users must:

- only use licensed software officially installed, registered and owned by the Society on Society provided devices.
- only use the applications to which they have authorised access
- comply with the terms of license signed by the Society for online databases, software programs, and online software packages
- ensure that all copyright material is only copied or used with the permission of the copyright owner, under the terms of a copyright licensing agreement, or as permitted by law.

28. The Technology Services team may periodically audit software installations to assess compliance with this policy. Users must respond to requests from the Technology Services team to provide evidence of software licences for non-standard software installed.

29. Ownership of all work product created by Society Personnel is assigned to the Society, or (if it is not capable of assignment) is exclusively licensed by the relevant Society Personnel to the Society for all purposes, and must not be used for purposes other than for the Society unless authorised by the Society's prior written consent.

Storage of data

30. Users are responsible for any data stored locally on Society devices (such as laptops, tablets or mobile phones). Data stored locally cannot be recovered if a device is lost, exchanged or a local storage fails or is erased.

31. Users must:

    - store all business data in the appropriate shared location (such as Teams, SharePoint etc.) as provided or approved by the Society and regularly manage documents in shared locations and delete files and folders that are no longer required in line with the Records Management Policy

32. Users must not:

    - use shared locations to store personal media files (such as photos, music and movie files). The Technology Services team may delete any personal media files stored in shared locations after two business days' notice by email to the owner of the files if the owner can be identified
    - keep multiple copies of the same document in different locations, unless they are required to be available offline, in which case users must use a replication technology like OneDrive.

Information Security Incidents

33. The Society has a Data Breach Response Plan for the timely and effective handling of information security incidents.

34. An information security incident is a suspected or confirmed event that poses a threat to the Society's Information Services. Information security incidents can originate from intentional (deliberate action against an information system) or unintentional action (human errors). An information security incident may cause a violation of the integrity, availability or confidentiality of the Society's information. Examples of potential information security incidents include:

- abnormal computer behaviour, which might be caused by a computer virus, malware, or worm
- disclosure of information to an unauthorised person
- lost or stolen physical access cards, removable media, laptops and passwords
- unauthorised access to an information system or physical premises.

35. Users must:

    - report any suspected information security incident or inappropriate material immediately to the Society's Technology Services Service Desk and their line manager. Ideally this report should be made by phoning the technology services desk.

    - Follow the instructions of the Technology Services desk, who will advise what steps should be taken to minimise the risk of a potential breach spreading throughout the network.

36. Users must not:

    - perform an action (e.g. delete system files) to eradicate or contain a suspected security incident unless explicitly instructed by the Service Desk or Security team
    - leave portable devices unattended and unlocked in public, even in a Society location
    - use unencrypted removable media (e.g. USB drives, external hard drives, CDs/DVDs) to store the Society's internal or external confidential information
    - use any personal removable media for business use, unless you are explicitly authorised to do so by the Society's Information Security Officer (ISO)
    - disclose information about security incidents to unauthorised entities.

Access to personal files and removal of unacceptable material

37. The Society may, without notice or employee approval, investigate, forensically capture and/or remove any illegal or unacceptable material from its computing resources.

User access and password security

38. All users will be provided with a secure individual account.

39. Users are responsible for the use of their account and must:

    - select and use strong passwords. It is recommended that passwords contain at least one Upper Case, one Lower Case, one number and one Special Character. It is important that passwords can be remembered. Passphrases (e.g. ILove2Work@Vinnies) can be easier to remember.
    - change their password every 120 days and/or if they suspect that their account has been compromised, or when requested by the Service Desk team to do so. Users should not change passwords within a three-day period after their last change.
    - use multi-factor authentication (MFA) on their Vinnies accounts wherever MFA is available. . Passphrases are still recommended with MFA as they are easier to remember and more secure. Personnel can contact the Service Desk for assistance to set up MFA.

- store passwords in a secure password location and not use post-it notes, Microsoft Excel, Outlook, OneNote and Word to store their passwords. The Society's selected secure password stores are Keepass and LastPass
- report any suspected compromise of passwords or PINs to the Technology Services Service Desk who will assist you in securing the affected user account

40. The password must not be based on anything that can be easily guessed or obtained using collateral information. The following must be avoided:

    - passwords related to names, dates of birth, telephone numbers, spouse or family members names or other family information
    - passwords used for any other email account
    - common words or terms relating to the Society or any of its services
    - common words found in dictionaries

41. Users must not:

    - reuse previous passwords. A history of the 10 last passwords is maintained by the system to prevent re-use
    - reveal their passwords under any circumstances
    - attempt to use any account other than their own
    - share their user account with other individuals including the Service Desk
    - use a shared user account unless specifically authorised by the Service Desk to do so as an exception.

Monitoring and Surveillance

42. The Society may monitor and record calls to the Service Desk at random for service quality, performance, training, monitoring purposes via audio tracking and other forms of tracking.

43. The Society will restrict access to an internet site or the delivery of an e-mail where access to the site or delivery of the e-mail conflicts with this policy.

44. The Society carries out computer surveillance on an ongoing basis to monitor the appropriate use of Information Services provided by, or on behalf of, the Society. Users should not store highly sensitive personal information on the Society's systems with an expectation of absolute privacy.

45. Routine computer surveillance includes:

    - monitoring visited internet sites
    - monitoring your use of e-mail and other electronic messaging systems
    - accessing and recording documents and other electronic records for the purposes of:
        - complying with legal obligations
        - audits and investigations and as a result of technical measures carried out for the purpose of managing the Society's Information Services
        - auditing data storage locations for inappropriate material.

46. The Society conducts surveillance of electronic devices in accordance with this policy, the *Workplace Surveillance Act 2005* and the *Privacy Act 1988* (Cth).

47. Users must not carry out their own surveillance under any circumstances. Technology Services will carry out all surveillance, under the control of the relevant Legal and Employment Relations representatives.

Confidentiality

48. Even though users may have access to a document or e-mail message created, received or stored using the Society's Information Services, users must treat them as confidential. Users may only read or use them if:

- they are the author or an intended recipient
- they are required to read or use them for a legitimate business purpose
- they are the authorised delegate of someone who is authorised to read or use the document or email
- they are the manager of a person who has left the Society and they are monitoring that inbox for business purposes.

49. Users should always consider their surroundings when accessing or discussing sensitive or confidential information to prevent inadvertent disclosures. Public locations such as cafes and public transport pose a higher risk of accidental leaks.

Travel

50. To protect the Society's information, society personnel should consider whether it is necessary to take a device owned by the Society when traveling outside Australia. Where this is necessary for work purposes, approval must be sought from the appropriate Director before travelling internationally.

51. All users who use the Society's technology overseas must contact the Service Desk before they are re-connected to the Society's network. The Service Desk will conduct relevant safeguards to reduce the risk of virus infection.

Leaving the Society

52. This section applies when users:

- leave the Society permanently
- commence a period of leave in excess of 60 days.
    - Users' Society login and e-mail account will be disabled and telephone account will be disabled.
    - Between the time users leave and the time that their accounts are disabled, their President, Team Leader, Manager, any of their delegates may have access to and control over their emails.

53. An Executive Director may approve an exception for staff on extended leave as appropriate.

Control Exceptions

54. All exemption requests must be reviewed and assessed by the Information Security Officer and approved by the Chief Information Officer.

Review

55. This policy is scheduled for review two years from its date of approval or more frequently as needed to align with legislative or other changes.

56. The effectiveness of the operation and communication of this policy is to be evaluated and reviewed by the Information Security Officer.

Further assistance

57. Users should direct queries regarding this policy to their line-manager or President.

58. Further assistance can be sought from the Information Security Officer.

Roles and responsibilities

Role	Responsibility
All Users	▪ Comply with this policy and related procedures ▪ Advise the ICT Service desk promptly regarding any loss of technology, system issue or potential breach of the Society's technology integrity ▪ Backup personal data on a regular basis ▪ Be aware that technology may be wiped completely of its data if lost or stolen ▪ Have the approval of your manager, President or Recruitment coordinator before being granted access to the Society's Technology
Presidents	▪ Ensure that all members reporting to them, with access to Society technology are familiarised with this policy (including completing the acknowledgement form at Appendix 3) and are notified of updates to this policy
Executive Directors	▪ Read this policy in conjunction with the Information Security Policy ▪ Acquire and update their knowledge of Information Communication Technology (Technology) matters ▪ Communicate changes in this policy to staff ▪ Ensure that the Society has appropriate processes in place to receive and respond promptly to potential and actual breaches of Technology security ▪ Ensure all Society personnel reporting to them are aware of and compliant with this policy (including completing the acknowledgement form at Appendices 3 and 5 as appropriate)
Regional Directors	▪ Ensure Conference members within their region who are issued with Society technology are familiarised with this policy

	during induction (including completing the Acceptable Use of Technology acknowledgement form at Appendix 3), and are notified of updates to this policy
Managers	▪ Read this policy with the Information Security Policy ▪ Ensure all employees and volunteers reporting to them are familiarised with this policy during induction (including completing the acknowledgement form at Appendix 3) and are notified of updates to this policy ▪ Monitor compliance with the Acceptable Usage Policy ▪ Support employees under their supervision to abide by this IT usage document, including: o ensuring employees are adequately trained and aware of their responsibilities o seeking authorisation for new Users from the Executive Director, Chief Financial Officer or delegate o advising the IT Service Desk of the authorisation of new Users o advising the IT Service Desk of any change in status or the departure of a User ▪ Actively ensure that any changes in legalisation, regulation or the Society's environment are incorporated into this Policy and Procedures
Chief Information Officer	▪ Approve control exemptions ▪ Ensure all users are notified of changes to this policy
Information Security Officer	▪ Ensure data security within the Society ▪ Ensure technology solutions, which prevent internal and external malicious users from compromising data integrity, are in place ▪ Review Control exemption requests

References

59. *Copyright Act 1968* (Cth)

60. *Privacy Act 1988* (Cth) and the Australian Privacy Principles (APPs) under that Act.

61. *Spam Act 2003* (Cth)

62. *Workplace Surveillance Act* 2005 No 47 NSW

Approval and amendment history

Version	Approval authority	Date	Amendment summary
Version 1	CIO	20.01.2018	NA
Version 2	Information Security Officer	24.09.2019	
Version 3	Information Security Officer	27.11.2019	
Doc # PO2019-009	Executive Leadership Team and State Council	03.12.2019	Format aligned with SVDP NSW policy framework. Incorporation of LAC ICT Usage Policy and Procedures.
Doc # PO2019-009 Version 2	Executive Director Corporate Services	27.07.2020	Updated ownership and responsibilities to align with organisational structure changes.
Doc#PO2021-009	Executive Leadership Team	29.09.2021	Policy reviewed in line with review cycle.
Doc#PO2022-009	Executive Leadership Team State Council	29.09.2021 19.02.2022	Policy reviewed in line with review cycle.

Appendix 1: Definitions

63. Relevant definitions include:

Term	Definition
Audio and Video Streaming	A method of sending video, music and voice data over the Internet in a constant stream so that people do not have to download a large file before they view or listen to it and includes services like YouTube, Spotify or similar services.
Computer Surveillance	Computer surveillance means surveillance by means of software or other equipment, which monitors or records the information input or output, or other use, of a computer.
Computer Systems	Communications facilities and associated equipment provided by the Society or in use at the Society offices, including mobile phones, and the use of SMS, Multimedia Message Services, video conferencing and instant messaging.
CRM	Contact management software.
Electronic Identity	Refers to the unique User identity defined by a user-name, e-mail address or telephone number and password of PIN combination by which you gain access to the supplied Technology. This also includes the use of Fingerprint security on mobile devices.
E-mail	The sending of messages and file attachments through the Society's networks.
Employee	An employee is a person who is hired to provide services in exchange for compensation (pay) (Australian Taxation Office, 2012). An employee is a paid member of staff – this can be on a full-time, part-time, fixed term or casual basis. The Rule (Part III, 2012, Article 26) describes the role of employees in a way that clearly refers to paid persons as 'employees, this includes contractors providing services to the Society for a set time or specific task and those engaged in the performance of duties for the Society from a labour hire agency.
Executive Director	A member of the Executive Leadership Team with the title Executive Director or Chief Financial Officer.
Health information	Information about physical or mental health or a disability an individual has had at any time, an individual's express wishes about future provision of health services, any health service that has been or is to be provided to an individual, any personal information collected to provide or in providing a health service, information collected in connection with a donation or intended donation of body parts, organs or body substances, genetic information that is

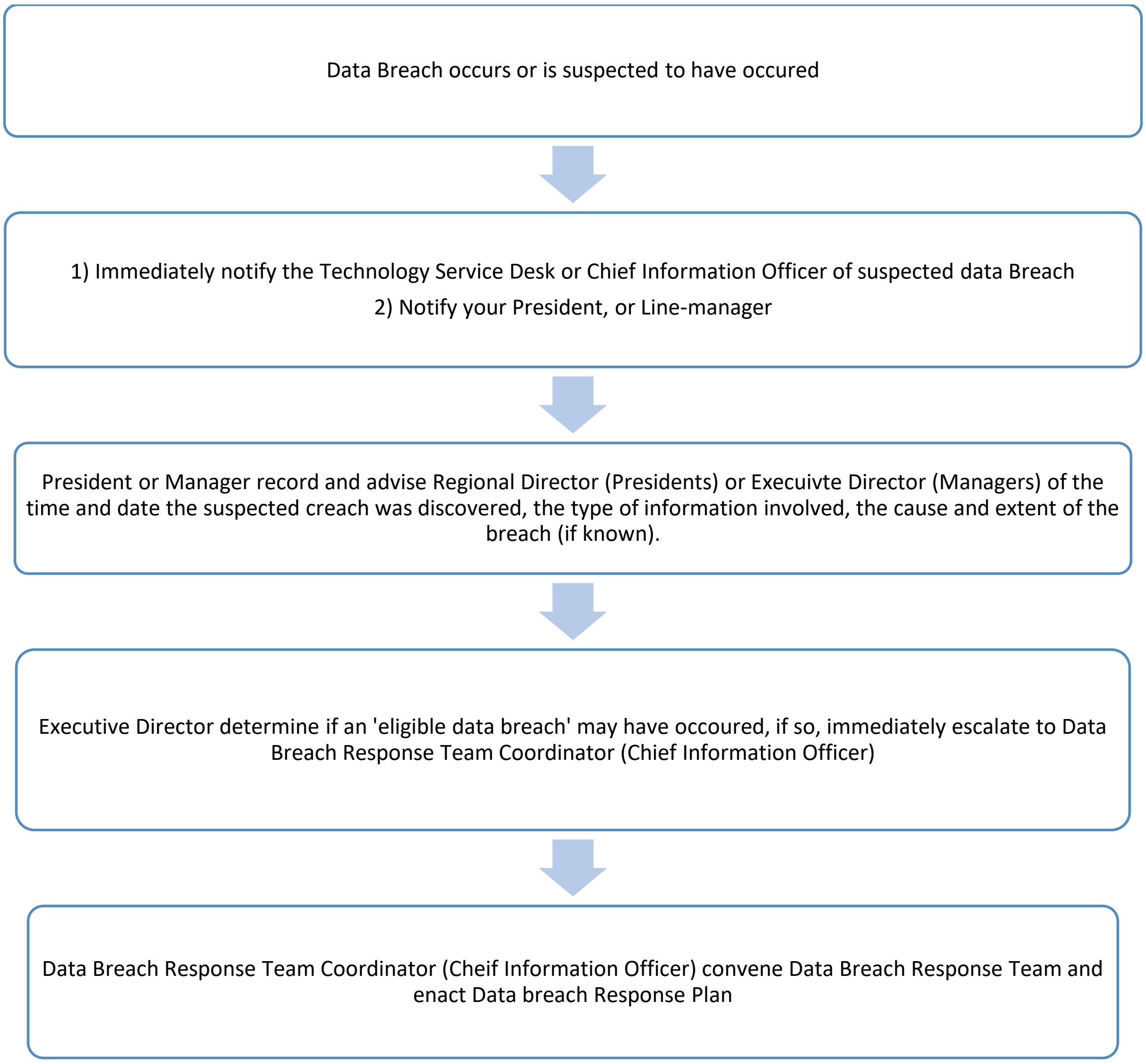
	or could be predictive of health at any time of the individual or a relative of the individual and healthcare identifiers.
Internet	The use of the Internet/intranet through the Society's computer networks.
Member	Conference, associate and volunteer members as per The Rule. Volunteer Members are registered as such by a procedure established by State Council.
PIN	Personal Identification Number.
President	A member elected to the position of President including conference President, Regional Council President, Central Council President and State Council President.
Personal Information	Information in electronic or hard copy form that either personally identifies, or can be used to reasonably identify, an individual (including their name, address, telephone number, email address, date of birth, signature, salary and banking details). It includes health and sensitive information,
Sensitive Information	A type of personal information and includes information about health, genetics, race, political opinion or membership, religion, philosophical beliefs, union membership, sexual preference and criminal record.
Society Personnel	Any person (or group of people) engaged by the Society to assist in its works. This includes members, volunteers, employees, contractors and consultants.
User	Includes all people who have access to the Society's Information Services including society personnel who are provided with an electronic identity (e.g. a username and password).
Volunteer	Persons who perform unpaid work for the Society (including students, interns, corporates, 'work for the dole' and 'community service order' participants).

Appendix 2: Suspected Data Breach Escalation Procedure

64. A data breach is an unauthorised access, modification, disclosure, loss or other misuse or interference to confidential information or information security controls.

65. A data breach can include:

- a viral infection
- mistakenly sending information to the wrong email addresses
- a computer hacking incident
- sharing information with a third party or supplier that is not security cleared by the Technology Services team
- a loss of a device with confidential information on it
- any other way that confidential information may have been lost or shared with an unintended recipient.



Data Breach occurs or is suspected to have occured

1) Immediately notify the Technology Service Desk or Chief Information Officer of suspected data Breach

2) Notify your President, or Line-manager

President or Manager record and advise Regional Director (Presidents) or Execuivte Director (Managers) of the time and date the suspected creach was discovered, the type of information involved, the cause and extent of the breach (if known).

Executive Director determine if an 'eligible data breach' may have occoured, if so, immediately escalate to Data Breach Response Team Coordinator (Chief Information Officer)

Data Breach Response Team Coordinator (Cheif Information Officer) convene Data Breach Response Team and enact Data breach Response Plan

Appendix 3: Acceptable Use of Technology Policy Acknowledgement

- I have received, read and understood the Acceptable Use of Technology Policy
- I agree to comply with the Acceptable Use of Technology Policy
- I understand that the Society undertakes continual computer surveillance and that reading this policy constitutes receiving notice of computer surveillance in accordance with the *Workplace Surveillance Act* 2005
- I understand that the Society may at any time vary its Acceptable Use of Technology Policy and I have a responsibility to read and comply with applicable policies
- I understand that my signed acknowledgement will be kept on my personnel or Society People file
- I have had the opportunity to ask any questions in order to clarify any issues in the Acceptable Use of Technology Policy
- I understand that if I breach any of the policy or procedures contained therein, I may face legal or disciplinary action according to any applicable law or Society Policy.

Print Name: …………………………………………...................

Signature: ……………………………………………………….

Date: ……………………......

Please return this to your President or Manager

Internal use only

Forms completed by employees should be returned to Employment Relations for adding to personnel files.

Forms completed by volunteers or members should be recorded in their Society People profile.