

Responsible Officer

Directorate

Executive Manager Governance and
People

Governance and People

Table of Contents

1.	Purpose and scope.....	2
2.	Legal framework and definitions	2
3.	Privacy governance and accountability	4
4.	Information Council holds	5
5.	Compliance with the IPPs and HPPs.....	6
6.	Public registers and suppression.....	7
7.	Access to and amendment of information	8
8.	Privacy complaints and internal review.....	9
9.	Mandatory notification of data breaches.....	9
10.	Digital services, cloud, AI and automated decision-making.....	10
11.	Contractors, data sharing and related bodies.....	11
12.	CCTV, engagement and special information handling.....	11
13.	Exemptions, confidentiality, misuse and offences	12
14.	Training, assurance, monitoring and review	13
15.	Contacts and related resources.....	14
	Appendix A: Public register access declaration.....	16
	Appendix B: Privacy collection notice template	17
	Appendix C: Access or amendment request	18
	Appendix D: Privacy internal review application	19
	Appendix E: Privacy impact screening checklist	20
	Appendix F: Data breach immediate action card.....	21

1. Purpose and scope

This Plan explains how Coonamble Shire Council manages personal and health information, complies with NSW privacy law, supports councillors and workers to make sound privacy decisions, and enables individuals to access, correct or complain about the handling of their information.

1.1 Statutory status

Section 33 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) requires Council to prepare and implement a Privacy Management Plan. The Plan describes Council's policies and practices for complying with the PPIP Act and *Health Records and Information Privacy Act 2002* (HRIP Act), how those practices are communicated, internal review procedures, and procedures and practices for Part 6A mandatory notification of data breaches.

If this Plan is inconsistent with legislation, a binding privacy code, public interest direction, order or court decision, the higher authority prevails. The Plan does not create or remove legal rights or obligations beyond those applying at law.

1.2 Application

- Councillors, employees, agency staff, volunteers, committee members, contractors, consultants and service providers handling information for Council.
- All Council functions, facilities, businesses, services, projects, websites, applications and systems.
- Personal and health information in any format, including paper, email, audio, images, CCTV, databases, mobile devices, cloud services, backups and information inferred through analytics or AI.

1.3 Commitment

- Privacy by design and default.
- Lawful, necessary and proportionate handling.
- Data minimisation and need-to-know access.
- Clear notice and accountable decision-making.
- Security throughout the information lifecycle.
- Respectful, accessible complaint and review pathways.

2. Legal framework and definitions

2.1 Principal legislation and instruments

- *Privacy and Personal Information Protection Act 1998* (PPIP Act).
- *Health Records and Information Privacy Act 2002* (HRIP Act).

- Information and Privacy Commission *Privacy Code of Practice for Local Government*.
- *Government Information (Public Access) Act 2009* (GIPA Act).
- *Local Government Act 1993, State Records Act 1998, Environmental Planning and Assessment Act 1979, Public Interest Disclosures Act 2022, Workplace Surveillance Act 2005, Surveillance Devices Act 2007* and any other laws applying to Council functions.

2.2 Definitions

Term	Meaning
Collect	Acquire information, whether actively sought, directly received or otherwise obtained.
Data breach	Unauthorised access to or disclosure of personal information, or loss in circumstances likely to result in unauthorised access or disclosure.
Disclose	Make information known to a person or body that did not already know it and is not authorised to receive it.
Eligible data breach	A breach satisfying Part 6A of the PPIP Act, including that a reasonable person would conclude the access or disclosure is likely to result in serious harm.
Health information	Information of a kind defined in section 6 of the HRIP Act, including information about health, disability and health services.
Personal information	Information or an opinion about an individual whose identity is apparent or can reasonably be ascertained, subject to exclusions in section 4 of the PPIP Act.
Sensitive information	Information requiring heightened safeguards due to its content or potential impact, including health, financial, identity, cultural, political, religious, trade union and sexual activity information.
Use	Handle information within Council for a purpose.

3. Privacy governance and accountability

3.1 Responsibilities

Role	Responsibilities
Council and General Manager	Set expectations, approve the Plan and ensure reasonable capability and resources.
Privacy Contact Officer (Executive Manager Governance and People)	Provide advice; coordinate access, amendment, complaints and internal reviews; liaise with the IPC; maintain registers; oversee assurance; review high-risk proposals.
Public Officer (Executive Manager Governance and People)	Support statutory access and public register processes and act as alternate where designated.
ICT Lead (System and Network Administrator)	Implement information and cyber security, access controls, logging, backup, recovery and technical breach response.
Executive Leadership Team	Own business-area privacy risks and oversee compliance, training and remediation.
Managers	Apply this Plan, approve role-based access, ensure records and notices are adequate, and escalate incidents.
All officials and workers	Use information only for authorised duties, protect it, use approved systems and report suspected breaches immediately.
Contractors and providers	Meet contractual privacy, security, records, return/destruction and incident obligations.

3.2 Privacy impact assessment

Privacy impact screening must occur at the concept stage of any proposal that handles personal or health information. A documented Privacy Impact Assessment (PIA) is required where the proposal is likely to have a material privacy impact, including surveillance, biometrics, data matching, substantial data sharing, cloud migration, high-volume collection, AI or automated decision-making.

- Map information flows, purposes, legal authority and affected people.
- Assess necessity, proportionality, notice, consent where relevant, access, accuracy, security, retention, sharing, transborder and re-identification risks.
- Identify heightened impacts on children and vulnerable people.
- Consider less privacy-intrusive alternatives and consult where appropriate.
- Document controls, residual risk, accountable approval and review date.

- Repeat the assessment if scope, information, vendor or technology materially changes.

3.3 New policies, forms and contracts

Business units must consult this Plan when developing policies, forms, services, agreements and systems. The Privacy Contact Officer should review high-risk collection notices, data-sharing arrangements, contracts and projects. Complex matters may be referred for legal, cyber security or specialist advice.

4. Information Council holds

Council holds personal and health information reasonably necessary to perform its statutory and service functions. Examples are illustrative, not exhaustive.

People/function	Examples
Residents, ratepayers and owners	Identity and contact details, property, rates, payments, requests, complaints, claims, permits, applications, submissions and correspondence.
Planning, building and regulation	Applications, plans, submissions, inspection material, photographs, recordings, notices, evidence and enforcement records.
Community services	Library and booking records, grants, events, access needs, surveys, mailing preferences and community support.
Councillors and committees	Contact details, disclosures of interests, expenses, training, conduct matters and meeting participation.
Employees, applicants and volunteers	Recruitment, payroll, banking, leave, health, workers compensation, performance, conduct, training and emergency contacts.
Digital services and security	Online forms, account identifiers, network and device logs, CCTV, access-control logs and incident records.
Integrity and legal	Complaints, public interest disclosures, investigations, legal advice, claims, subpoenas and protected information.

4.1 Unsolicited information

When unsolicited personal or health information is received, Council will consider whether it could lawfully have been collected and whether retention is necessary. Information not required will be securely destroyed or de-identified where lawful and consistent with records obligations. If retained, the storage, use, disclosure, access and security principles apply.

4.2 Publicly available information

Information in a publicly available publication may be excluded from the PPIP Act definition of personal information. This does not mean all information available somewhere online may be freely reused. Council must verify the source, purpose, accuracy, legal authority and any confidentiality, safety, copyright or other restrictions before use or disclosure.

5. Compliance with the IPPs and HPPs

Council applies the 12 Information Protection Principles and 15 Health Privacy Principles, subject to lawful exemptions and the Privacy Code of Practice for Local Government.

Principle	Council practice
Lawful purpose, IPP/HPP 1	Identify the Council function, authority and need. Do not collect information merely because it may later be useful.
Direct collection, IPP/HPP 2	Collect directly unless consent or a lawful exception applies, or direct collection of health information is unreasonable or impracticable.
Notice, IPP/HPP 3	At or before collection, explain Council identity, purpose, recipients, mandatory or voluntary supply, consequences, storage and access/correction pathways.
Relevant and non-intrusive, IPP/HPP 4	Collect accurate, relevant and not excessive information using proportionate methods.
Retention and security, IPP/HPP 5	Use risk-based physical and digital safeguards; retain and dispose under authorised records rules and legal holds.
Openness and access, IPP/HPP 6-7	Explain holdings and provide access without unreasonable delay or expense, subject to lawful limits.
Amendment, IPP/HPP 8	Correct or annotate information so it is accurate, relevant, current, complete and not misleading.
Accuracy before use, IPP/HPP 9	Use current authoritative records and verify material facts where decisions may significantly affect a person.
Limited use, IPP/HPP 10	Use for the collection purpose, a directly related purpose, with consent or another lawful basis.
Limited disclosure, IPP/HPP 11	Disclose with consent, reasonable expectation and related purpose, or another lawful authority. Verify identity and disclose the minimum necessary.

Special/transborder limits, IPP 12; HPP 14	Apply special statutory restrictions to sensitive information and transfers outside NSW. Assess recipient protections, location, contracts and controls.
Identifiers/anonymity/linkage, HPP 12-15	Use identifiers only where necessary; offer anonymity where lawful and practicable; obtain express consent for health-record linkage unless otherwise authorised.

5.1 Collection notices

A transaction-specific collection notice must be provided at or before collection and tailored to the information flow. A general website privacy statement does not replace a collection notice. Appendix B provides a template.

5.2 Practical security measures

- Use approved systems, accounts and storage. Do not use personal email, consumer file sharing or unapproved AI for Council personal information.
- Use BCC for bulk external email unless visibility is expected and lawful. Check recipients and attachments before sending.
- Protect passwords and authentication codes; lock screens and secure paper records.
- Grant least-privilege access and promptly amend or remove access when duties change or employment ends.
- Use secure transfer and maintain auditable records for high-risk access and disclosure.
- Apply authorised retention and secure disposal. Do not retain convenience copies beyond need.
- Provide contractors only the minimum information and access necessary.

6. Public registers and suppression

A public register is a register of personal information required by law to be, or made, publicly available or open to public inspection. Council will maintain an internal schedule specifying each register, enabling law, statutory purpose, access method, responsible unit and restrictions.

6.1 Access to public registers

1. Confirm that the record is a public register and identify its statutory purpose.
2. Obtain sufficient particulars of the intended use. Council may require a statutory declaration.

3. Assess whether the proposed use relates to the purpose of the register or its enabling Act.
4. Disclose only the minimum information required. Bulk access, sale, scraping or access to a substantial part of a register requires heightened assessment.
5. Record the decision, information disclosed and any conditions.

6.2 Council registers

Depending on current legislation and Council holdings, public registers may include records relating to Council land, approvals, disclosures of interests, development consents and certificates, building certificates, licences and impounding. The responsible officer must verify current legislative requirements before access is given. The rates record is not a public register merely because Council holds it.

6.3 Suppression

Under section 58 of the PPIP Act, a person may seek suppression where non-suppression would affect a person's safety or wellbeing. Section 739 of the Local Government Act may also apply to certain residential address information. Council will assist the applicant, accept relevant evidence, restrict access while assessing urgent risk, weigh any countervailing public interest, give reasons and explain review pathways.

7. Access to and amendment of information

A person may ask whether Council holds personal or health information about them, request access, or seek amendment. Council will use the simplest suitable administrative, PPIP Act, HRIP Act or GIPA Act pathway and explain the chosen process.

7.1 Identity and authority

- Verify identity proportionately and avoid retaining unnecessary identity evidence.
- A representative must establish their identity and authority, such as written authority, guardianship or power of attorney.
- Consider third-party information, privilege, confidentiality, safety, investigation material and other legal restrictions.
- Where full access is unavailable, consider lawful redaction, partial access, a summary or supervised inspection.

7.2 Amendment

Council will assess whether information is accurate, relevant, current, complete and not misleading for the purpose for which it is held. Where a requested amendment is not made, Council will provide reasons and, where required, permit a statement of the requested correction to be associated with the record. Relevant recipients may be notified of a correction where appropriate.

8. Privacy complaints and internal review

8.1 Informal complaints

Minor concerns may be resolved promptly under Council's complaints arrangements where the person agrees. Informal handling does not remove the right to seek formal internal review within the statutory time limit. Staff must not discourage or obstruct an application.

8.2 Internal review

A person may apply for internal review if they consider Council has breached an IPP, HPP, applicable privacy code or public register provision. The application should be written, include an Australian address for notices, describe the conduct and ordinarily be lodged within six months after the person became aware of it. Council may accept a late application.

1. Register and acknowledge the application.
2. Notify the NSW Privacy Commissioner as soon as practicable.
3. Appoint a suitably senior and independent reviewing officer with no conflict of interest.
4. Gather records, provide procedural fairness, consider IPC submissions and apply current legislation and guidance.
5. Complete the review within 60 days.
6. Notify the applicant of findings, reasons and action within 14 days after completion, and notify the Privacy Commissioner.
7. Record outcomes, protect confidentiality, implement corrective action and report trends appropriately.

8.3 Outcomes and external avenues

- No further action; apology; access or amendment; change to a practice, system or training; undertaking not to repeat conduct; or other appropriate action.
- A person may complain to the Privacy Commissioner under section 45 of the PPIP Act.
- A person may apply to NCAT where statutory requirements are met. Council will provide current contact information and explain applicable review avenues.

9. Mandatory notification of data breaches

Council must maintain and publish a standalone Data Breach Policy under section 59ZD of the PPIP Act. This Plan describes its relationship with Council's broader privacy framework and does not replace that policy.

9.1 Reporting and response

All suspected loss, unauthorised access or unauthorised disclosure must be reported immediately to the Privacy Contact Officer and ICT lead through Council's incident process. Staff must safely contain within their authority, preserve evidence and avoid deleting relevant records.

1. Triage and contain the incident.
2. Assess reasonably and expeditiously under Part 6A, having regard to IPC guidelines, information sensitivity, security, affected individuals and likely serious harm.
3. Mitigate harm and correct control failures.
4. Notify the Privacy Commissioner and affected individuals as soon as practicable if an eligible data breach has occurred, unless a statutory exemption applies.
5. Where direct notification is not reasonably practicable, issue public notification and maintain the Public Notification Register as required.
6. Maintain the internal eligible data breach register and complete a post-incident review.

9.2 Contractors and multiple agencies

Contracts must require immediate incident reporting, evidence preservation, access to relevant logs, containment, assessment support, notification cooperation and remediation. Council remains responsible for its statutory obligations for information held on its behalf. Where more than one agency is involved, Council will coordinate roles while ensuring its own obligations are met.

9.3 Publication and review

Council's Data Breach Policy and Public Notification Register must be readily discoverable on its website. The Data Breach Policy should be reviewed in accordance with its document control provisions and after a material incident or exercise. Council will periodically test its response arrangements.

10. Digital services, cloud, AI and automated decision-making

10.1 Cloud and digital platforms

Before approval, Council will assess data location, subcontractors, access, encryption, logging, retention and deletion, backup, incident response, export, legal access risk and exit arrangements. Controls and approval must be proportionate to sensitivity and scale.

10.2 Generative AI

- Do not enter personal, health, confidential, privileged, security-sensitive or protected information into an AI service unless the service and use case are formally approved and controls documented.
- Complete privacy impact screening and a PIA where personal information or a material decision is involved.
- Verify outputs for accuracy, completeness, bias and inappropriate disclosure. Capture validated records in Council's records system.
- Do not use personal information to train or fine-tune a model without clear authority, necessity, approval and appropriate notice.
- Maintain meaningful human oversight for decisions affecting rights, services, compliance or enforcement.
- Be transparent where AI materially affects a service, communication or decision, subject to lawful security limits.

10.3 Automated decision-making

Where automated decision-making uses personal information, Council will explain the system purpose, information used, decision type, material effect, safeguarding, sharing, access and correction pathways and how a person can seek effective human review. Council will test accuracy and fairness, monitor impacts and retain an appropriate audit trail.

11. Contractors, data sharing and related bodies

11.1 Contract controls

- Defined purpose, permitted handling and minimum access.
- Compliance with privacy, records and Council requirements.
- Security, personnel, subcontracting, offshore access, secondary use and model-training restrictions.
- Immediate breach reporting and cooperation with Council and regulators.
- Audit, assurance, continuity, export, return, deletion and exit rights.
- Continuing confidentiality and privacy obligations after termination.

11.2 Data sharing

Before sharing information, Council will document purpose, authority, necessity, minimum fields, recipient, security, retention, onward disclosure, notice, accuracy, breach handling and review arrangements. High-risk or recurring sharing should be supported by an agreement and PIA. De-identified or aggregated information is preferred where it meets the purpose, but re-identification risk must be considered.

12. CCTV, engagement and special information handling

12.1 CCTV and surveillance

Council may use CCTV and authorised surveillance for lawful purposes including safety, asset protection, incident management, crime prevention and investigation. Images,

recordings and metadata may be personal information and must be handled under this Plan, surveillance legislation and Council's applicable CCTV policies.

- Use surveillance only for a defined, necessary and proportionate purpose.
- Provide prominent notice where required and practicable.
- Limit and audit access to authorised personnel.
- Retain for the authorised period or while required for a legal hold, incident or proceeding.
- Record lawful disclosure to police, insurers, investigators or other recipients.
- Complete privacy screening for new or materially changed surveillance.

12.2 Engagement, submissions, petitions and events

Collection notices will explain foreseeable publication or inclusion in business papers. Council will ordinarily remove unnecessary contact details, signatures and sensitive information before publication, while considering the GIPA Act, meeting requirements, safety, confidentiality, copyright and defamation. Surveys and outreach will use anonymous or aggregated information where suitable and avoid collecting unnecessary sensitive information.

12.3 Complaints, investigations and PIDs

Complaint, investigation and public interest disclosure material must be restricted to authorised personnel. Council will balance notice and access requirements with lawful confidentiality, safety, procedural fairness, investigation and PID protections. The exclusion of some PID information from the PPIP Act does not remove Council's security, records and protection obligations.

12.4 Councillor and workforce information

Health, payroll, recruitment, conduct, performance, workers compensation, disclosure-of-interest and similar records require heightened access controls. Workplace surveillance must comply with the Workplace Surveillance Act, applicable notices and Council policies.

13. Exemptions, confidentiality, misuse and offences

13.1 Exemptions and code modifications

The PPIP Act, HRIP Act, regulations, privacy codes and public interest directions contain exemptions or modifications that may apply in defined circumstances. Examples potentially relevant to Council include legal proceedings, law enforcement, public revenue, investigations, subpoenas and warrants, statutory authority, serious threats and circumstances where compliance would prejudice the individual's interests.

The Privacy Code of Practice for Local Government modifies specified IPPs and public register provisions, including for defined local-government activities. It is not a blanket exemption. The responsible officer must consult the current legislation and Code, ensure all

conditions are met and document material reliance. Complex or contested matters should be referred to the Privacy Contact Officer and, where appropriate, for legal advice.

13.2 Public interest directions

Before relying on a direction, Council must verify that it is current, covers the proposed conduct and that all conditions are met. Material reliance must be documented.

13.3 Confidentiality

Privacy and confidentiality overlap but are not identical. Confidentiality may arise from legislation, contract, equity, legal professional privilege, Council policy or circumstances. Authority to disclose confidential information does not necessarily authorise disclosure of personal information, and vice versa. Both questions must be considered.

13.4 Misuse and offences

Council officials, contractors and agents must not intentionally access, use, disclose or offer to supply personal or health information except as authorised for official duties. Unauthorised conduct may constitute misconduct, breach of contract, a privacy or computer offence, and may lead to disciplinary, civil or criminal action. Fixed penalty amounts are not reproduced because current legislation prevails.

- Report suspected deliberate misuse immediately through an authorised channel.
- Preserve evidence, manage any data breach and make required referrals.
- No person may threaten, intimidate, misrepresent or improperly pressure another person to prevent an access request, privacy complaint or internal review.

14. Training, assurance, monitoring and review

14.1 Training and dissemination

- Provide privacy induction to employees, councillors, volunteers and relevant contractors.
- Provide periodic refresher training on secure handling and breach reporting.
- Provide role-specific training for customer service, HR, planning, compliance, records, ICT, procurement, communications and complaint handling.
- Maintain training records and notify relevant personnel of material updates.
- Publish the Plan on Council's website and make it readily accessible internally and on request.
- Promote privacy awareness, including during Privacy Awareness Week.

14.2 Assurance

- Periodic business-unit review of forms, notices, holdings, access, retention and risks.
- Role-based access reviews for high-risk systems and repositories.
- Contractor and vendor assurance proportionate to risk.

- Sampling of information proposed for publication.
- Review complaints, access requests, incidents, near misses and trends.
- Test data breach response arrangements and track corrective actions.
- Report material privacy risks and overdue actions to ELT.

14.3 Review

The Privacy Contact Officer will review this Plan at least every two years and earlier following legislative or regulatory change, material IPC guidance, a significant incident, audit finding, major change in Council functions or adoption of high-risk technology. Following adoption, Council will provide the Plan to the NSW Privacy Commissioner and publish it.

15. Contacts and related resources

Organisation	Contact
Coonamble Shire Council	80 Castlereagh Street, Coonamble NSW 2829 PO Box 249, Coonamble NSW 2829 02 6827 1900 council@coonambleshire.nsw.gov.au www.coonambleshire.nsw.gov.au
Privacy Contact Officer	Executive Manager Governance and People, via Council contact details
Information and Privacy Commission NSW	1800 472 679 ipcinfo@ipc.nsw.gov.au www.ipc.nsw.gov.au
NSW Civil and Administrative Tribunal	1300 006 228 www.ncat.nsw.gov.au

15.1 Related Council documents

- Data Breach Policy and Public Notification Register.
- Code of Conduct and Procedures for the Administration of the Code of Conduct.
- Public Interest Disclosures Policy.
- Records management, information security, acceptable use, CCTV/surveillance, GIPA, complaints, procurement and contract management documents.

15.2 External guidance considered

- IPC Guide to making Privacy Management Plans and Privacy Management Plans Checklist, May 2026.
- IPC guidance and resources for the Mandatory Notification of Data Breach Scheme.

- IPC guidance on generative AI, automated decision-making, data sharing and Privacy Impact Assessments.
- Privacy Code of Practice for Local Government.
- NSW Ombudsman complaint management and procedural fairness guidance, where applicable.

Appendix A: Public register access declaration

Use this form where Council requires particulars of the intended use of personal information from a public register. A statutory declaration may be required depending on the request and Council's assessment.

Field	Applicant response
Applicant name and organisation (if applicable)	
Postal address	
Contact details	
Register and information requested	
Individual/s concerned	
Detailed intended use	
How the intended use relates to the purpose of the register	
Amount and format requested	
Proposed copying, publication, linkage, sale or further disclosure	
Declaration	I declare that the information supplied is true and that information obtained will be used only for the stated purpose and subject to any conditions imposed by Council.
Signature and date	

Appendix B: Privacy collection notice template

Coonamble Shire Council is collecting your [describe information] for [list the specific purpose/s] under/for [legal authority (eg name of Act) or Council function]. Providing [identify the type of information] is [required/voluntary]. If it is not provided, [state consequence/s]. Council will use the information for [list use/s] and may disclose it to [list any specific recipients] for [list purpose/legal basis]. Council will store it in [system/location]. You may request access to or correction of your information by contacting the Privacy Contact Officer on 02 6827 1900 or council@coonambleshire.nsw.gov.au. [Add any publication, cloud/offshore, AI, matching, surveillance or other material handling information.]

Collection notice checklist

- Specific lawful purpose and authority identified.
- Each field necessary and proportionate.
- Uses, recipients and publication stated.
- Mandatory/voluntary status and consequences stated.
- Storage and access/correction pathways stated.
- Notice provided at or before collection and in an accessible form.

Appendix C: Access or amendment request

Field	Applicant response
Applicant name	
Postal address	
Contact details	
Request: confirmation / access / amendment	
Information or record sought	
Date range and business area	
Preferred access format	
Requested amendment and reasons	
Supporting evidence	
Identity verification arrangements. Note: Council will advise what evidence is proportionate. Do not email identity documents unless requested through an approved channel.	
Representative and authority, if applicable	
Signature and date	

Appendix D: Privacy internal review application

Field	Applicant response
Applicant name	
Postal address for notices	
Contact details	
Date conduct became known	
Conduct or decision complained about	
Information involved	
Why privacy requirements may have been breached	
Impact	
Outcome sought	
Related reference and attachments (list)	
Signature and date	

Lodge with: Privacy Contact Officer, Coonamble Shire Council, PO Box 249, Coonamble NSW 2829, or council@coonambleshire.nsw.gov.au. Contact Council for assistance or an accessible format.

Appendix E: Privacy impact screening checklist

Question	Yes / No / Notes
New types or volumes of personal or health information?	
Children, vulnerable people or sensitive information?	
Surveillance, biometrics, matching, profiling, AI or automated decisions?	
External provider, cloud, subcontractor or offshore access?	
Material impact on rights, services, reputation or safety?	
Reliance on consent and is it valid?	
Less privacy-intrusive alternative available?	
Notices, security, retention, access and breach arrangements defined?	
Full PIA required, with approver and date?	

Appendix F: Data breach immediate action card

If personal or health information may have been lost, accessed or disclosed without authority:

1. Report immediately to the Privacy Contact Officer and ICT lead.
2. Contain safely within your authority, such as recalling email, revoking links, recovering documents or disabling compromised access.
3. Preserve evidence. Do not delete emails, logs, files or devices.
4. Record what happened, when, systems, people, information types, recipients and actions.
5. Do not contact affected people, media or other parties unless authorised by the response lead.
6. Support assessment, notification, remediation and post-incident review.

Report every suspected breach, even if it appears minor, was quickly contained or involves a contractor.