Fact Sheet

Updated August 2022

Digital records and the GIPA Act

This fact sheet has been developed to provide guidance about the definition of record, in particular digital records under the GIPA Act and what it means for agencies. The fact sheet also outlines the importance of agencies maintaining good digital recordkeeping practices to ensure it is able to comply with its legislative obligations.

The objective of the *Government Information (Public Access) Act 2009* (GIPA Act) is to promote the release of government information to the public. Under the GIPA Act, government information is defined as the information contained in a record held by an agency.[1]

Government information includes not only information contained in an agency's hard copy records but also information contained in an agency's electronic or digital records.

Agencies should be aware that government information contained in records in electronic or digital format are subject to access applications under the GIPA Act.

What is a record?

Under the GIPA Act a record includes any document or other source of information compiled, recorded or stored in written form or by electronic process, or by any other manner or by any other means.[2]

This means that in addition to paper or hard copy records, digital records can be the subject of a GIPA application, where that information is held by the agency.

The *State Records Act 1998* also defines record as any document or other source of information compiled, recorded or stored in written form or on film, or by electronic process, or in any other manner or by any other means.[3] Additionally, the State Records Act also defines a record in relation to its official nature, not just how it has been created or stored. The Act defines *state records* as those records which are made and kept, or received and kept …**in the course of the exercise of official functions.**"[4]

This means that any information created or received in the course of an officer's duties as a public servant, regardless of format or the technologies used, are records and must be managed in accordance with the *State Records Act*.

Types of digital records

Any Government information that is compiled, recorded or stored in a digital format or in a digital platform may be considered a record.

The following types of digital information are considered to be a record under the GIPA Act:

- SMS messages on a mobile phone;
- messages in WhatsApp;
- emails and any attachments;
- electronic copies of documents (including draft documents);
- contents within a database (such as a record or data in a business system or online application or software-as-a-service application);
- audit and access logs for business systems; and
- CCTV footage and other audio visual information.[5]

Digital records and new technology platforms

Increasingly, agencies are utilising new technologies and digital platforms to carry out their business or in providing services to the public.

For example, many agencies use a range of new digital platforms (including Twitter, Yammer and Microsoft Teams) as part of their business. Agencies should be aware that messages, forums and posts created using these platforms are digital records under the GIPA Act if they have been used for conducting government business.

Similarly, messages created in messaging apps (such as WhatsApp, Facebook Messenger and WeChat) are digital records if the messages have been used for conducting government business.

If an agency decides that these technologies are going to be used to conduct business within the agency or externally with clients etc, then the agency is creating digital records within these systems. The agency will need to determine how it will capture and store these records and make them available if required under the GIPA Act.[6]

[1] GIPA Act section 3(1)
[2] GIPA Act clause 10 of Schedule 4
[3] State Records Act section 3, definition of a record
[4] State Records Act section 3, definition of a State record

[5] For information about how the IPC considers audio visual information see IPC Fact Sheet: Managing access to audio visual information under the GIPA Act
[6] See *Redfern Legal Centre v Commissioner of Police* [2021] NSWCATAD 288 where the Tribunal held that because data

It is important that agencies have in place systems and governance arrangements that communicate to staff expectations and responsibilities associated with the use of these technologies under the GIPA Act.

Agencies should also keep in mind that under the *State Records Act*, they have a responsibility to ensure safe custody and proper preservation of State records under their control.[7]

When is a digital record not considered to be government information under the GIPA Act?

Not all digital records are classed as government information under the GIPA Act.

The GIPA Act states that government information is information contained in a record held by an agency or held by a person in his or her capacity as an officer of the agency.[8]

For example, an officer may access their personal email account on a device provided by the agency. Information contained in the officer's personal email account is not government information under the GIPA Act because:

- the agency does not hold the emails; and
- the emails are held by the officer in their personal capacity, not as an officer of the agency.

But if the officer conducts government business using their personal email account etc, then those emails are considered to be State records and must be returned to the agency. Using personal email accounts to conduct government business is strongly discouraged.

Increasingly as service delivery methods evolve, an agency may have an agreement with a private sector contractor to provide services to the public on its behalf. In these circumstances, the digital records held by the contractor may also be classified as government information under the GIPA Act even though the agency may not hold the record.[9] This is because the Agency has an immediate right of access under the GIPA Act. Agencies and contractors should be aware that access applications can be made for this information and plan accordingly.[10] The GIPA Act also outlines certain circumstances where information is not to be classified as government information held by an agency.

Government information in a record that is generally accessible to the public may not necessarily be classed as a record held by the agency. For example, information found on an agency's website is not government information held by an agency because it is available to the general public over the Internet.[11] However agencies should also be aware that where information is no longer publicly available, an access application can be made for that information.

Information received by an agency which is not solicited and not relevant to agency's business or functions will not be classified as government information held by the agency.[12]

When is a digital record not held by an agency?

A digital record may not always be held by an agency, despite the record containing information relating to an officer's duties.

In *Nolan v Commissioner of Police, NSW Police Force* [2019] NSWCATAD 120, the Applicant made an access application under the GIPA Act for access to call recordings made to and from an officer's personal mobile phone.

The Tribunal found that the GIPA Act did not require agencies to undertake searches for records that are outside the agency's electronic possession or control. While the call recordings may have contained information relating to the officer's official duties, the mobile phone was found to be under the possession and control of the officer in their personal capacity.

The Tribunal has recognised the relevance of the digital record environment to agency search requirements.[13] Agencies should make sure they know where to search when attempting to locate records for an access application. Additionally, agencies should ensure that any official government business is conducted through official business systems and captured within the Agency's recordkeeping systems. An agency may also create a new record to provide access to digitals records held but is not obliged or compelled to do so. In a digital government context, agencies must respond to the practical reality that all digitally created and stored information will require 'treatment' to some extent to bring it into existence.[14]

Managing digital records

To preserve the right of access to information in digital records agencies must consider:

- who holds the records;
- how access is provided; and
- in what form access can be provided.

was stored in a number, likely thousands, of tables on the COPS database, it was not held by NSW Police, which would have been required to write a Standard Query Language to extract the information

[7] State Records Act section 11(1)

[8] GIPA Act clause 12(1)(a)(d) of Schedule 4

[9] For more information on how agencies are required to deal with contractors see the IPC's Fact Sheet: Guide to section 121 of the GIPA Act for agencies

[10] The State Archives and Records Authority provides guidance on managing the outsourcing of Government functions and activities. For more information see Accountable Outsourcing

[11] GIPA Act clause 12(2) of Schedule 4

[12] GIPA Act clause 12(4) of Schedule 4

[13] *Miskelly v Roads and Maritime Services* [2019] NSWCATAD 133 at [97]

[14] For more information on creating new records see the IPC's Fact Sheet: Creating new records under the GIPA Act

To discharge their obligations under the GIPA Act, agencies are required to:

- conduct reasonable searches on electronic repositories to identify records that have been requested as part of an access application;
- make government information available to the public in digital or electronic format; or
- release digital records to applicants.

In addition, the State Records Act provides that agencies must make and keep full and accurate records of activities.[15] If a record is dependent on technology or equipment in order to access the record, then these records must be managed appropriately to ensure that access is possible now and into the future. This will usually mean migrating the records to new technologies or applications. This also will ensure that the information is able to be produced or made available under the GIPA Act in response to an access application.[16] Agencies also have a responsibility to safeguard and protect records over time.[17]

Agencies should manage their digital records in accordance with operational requirements and the *State Records Act*. Digital recordkeeping procedures and policies should take into account functions and activities, and be regularly reviewed and updated according to business needs.

Efficient day to day management of digital records can assist agencies when responding to access applications. Maintaining a consistent approach to handling records ensures agencies can easily identify, search and locate information.

The State Archives and Records Authority of NSW has issued Standard: No 12 Standard on records management. The Standard establishes requirements that agencies should follow in order to effectively manage their information and records.

Consistent with the Standard, agencies should consider:

- having policies in place to manage hardcopy and digital records;
- ensuring their records and information management policy supports the agency's activities;
- having systems in place to ensure that records are well managed; and
- ensuring access to records is provided in accordance with legislation including the GIPA Act.

Recordkeeping and the GIPA Act

For the purposes of the GIPA Act, an agency's digital recordkeeping procedures should include:

- ensuring officers are aware that digital records can be the subject of access applications under the GIPA Act;
- ensuring GIPA policies and procedures include references to both hardcopy and digital records;
- ensuring that policies and procedures set out clear business rules for the use of apps, social media and other similar tools;
- a governance framework around these technologies and establish rules for what is to be discussed in these technologies or collaborative spaces;
- training GIPA responsible officers on how to undertake reasonable searches in order to identify digital records;
- establishing clear business rules on how to correctly manage digital records to ensure there is a consistent approach to understanding and managing digital records agency-wide;
- regular refresher training to all staff on how to collect, handle, store and dispose of digital records and information; and
- having senior management and responsible officers champion good digital recordkeeping practices across the agency.

Retrieving digital records

The GIPA Act provides that an access application is to be determined within 20 working days, which can be extended up to 10 days if the agency is required to consult another party or retrieve archived records, or a maximum of 15 days where the agency has to both consult and retrieve archived records.[18]

The manner in which an agency routinely saves records, such as emails, to its normal electronic record keeping system does not ordinarily enliven the discretion to extend the decision period by 10 days. The process of retrieval from a records archive must involve some difficulty because an agency is required to undertake an act of retrieval from a place where public or historical records are kept, for the discretion to be enlivened.[19] Digital archives generally have the benefit of being easily accessible and searchable, therefore facilitating the quick retrieval of archived records.

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

Note: The IPC can give general advice on rights and compliance under the GIPA Act, but cannot give legal advice.You should seek your own legal advice about these issues.

[15] State Records Act section 12(1)
[16] State Records Act section 14(1)
[17] State Records Act section 11(1)
[18] GIPA Act section 57
[19] *Walton v Eurobodalla Shire Council* [2022] NSWCATAD 46