# Maintaining practice through policy in digital forensics and digital preservation

Martin Gengenbach

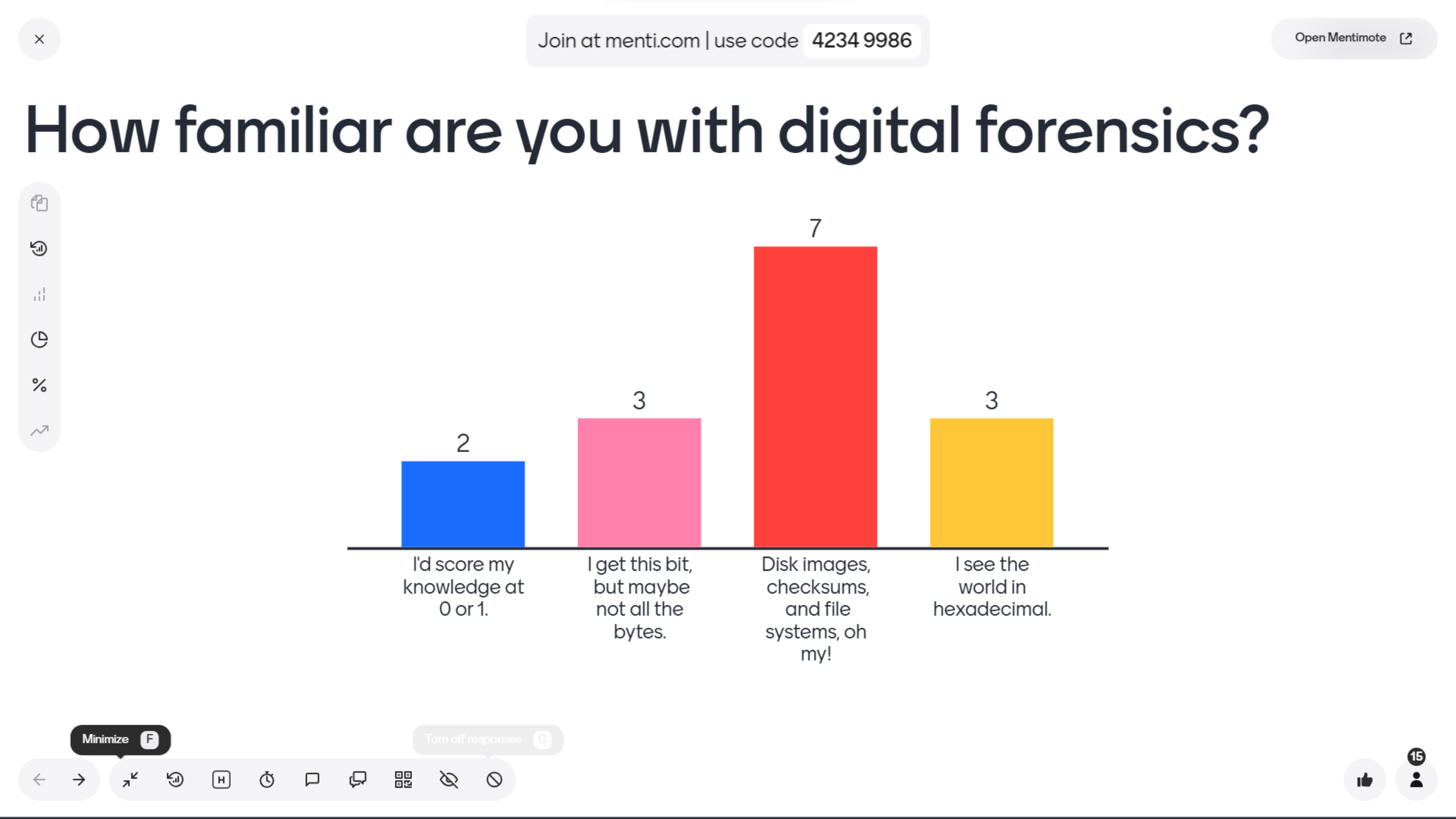
National Library of New Zealand

29 February 2024

# Acknowledgement

*Ki a koutou ngā maunga, ngā awa, ngā waka, ngā tupuna o Aotearoa me te Whenua Moemoea e huihui mai nei, tēnā koutou katoa.*

To you the mountains, rivers, waka, ancestors of Aotearoa and the Land of the Dreaming (Australia) that are gathered here, greetings to you all.



Join at menti.com | use code 4234 9986

# How familiar are you with digital forensics?

Open Mentimote
2
I'd score my knowledge at 0 or 1.
3
I get this bit, but maybe not all the bytes.
7
Disk images, checksums, and file systems, oh my!
3
I see the world in hexadecimal.
Minimize F
Turn off responses C
15

# Digital forensics

“Digital forensics is an **applied field** originating in law enforcement, computer security, and national defense. It is concerned with discovering, authenticating, and analyzing data in digital formats to the standard of admissibility in a legal setting. “

Digital Forensics and Born-Digital Content in Cultural Heritage Institutions (2013): https://www.clir.org/pubs/reports/pub149/

# Digital forensics

“‘forensics’ essentially refers to the process of in depth analysis of information that exists in the present, in order to reconstruct past events or objects, with the proffered interpretation being subject to scrutiny by others.”

Jeremy Leighton John, *Digital Forensics and Preservation* (DPC Technology Watch Report, 2012): https://www.dpconline.org/docs/dpc-technology-watch-publications/technology-watch-reports-1/810-dpctw12-03-pdf/file

# Digital preservation

Digital Preservation Refers to the **series of managed activities** necessary to **ensure continued access to digital materials** for as long as necessary ...(digital preservation) refers to all of the **actions** required to **maintain access to digital materials** beyond the limits of media failure or technological and organisational change.

DPC: What is Digital Preservation? [https://www.dpconline.org/digipres/what-is-digipres](https://www.dpconline.org/digipres/what-is-digipres)

# What is digital forensics in the context of digital preservation?

- Digital forensics provides tools and methods
- Digital forensics can be **applied** to achieve **goals** to support digital preservation (authenticity, chain of custody)
- Digital forensics tools and technologies can be used to **fulfil commitments** for how digital materials are to be handled (integrity, privacy

# Questions of the day

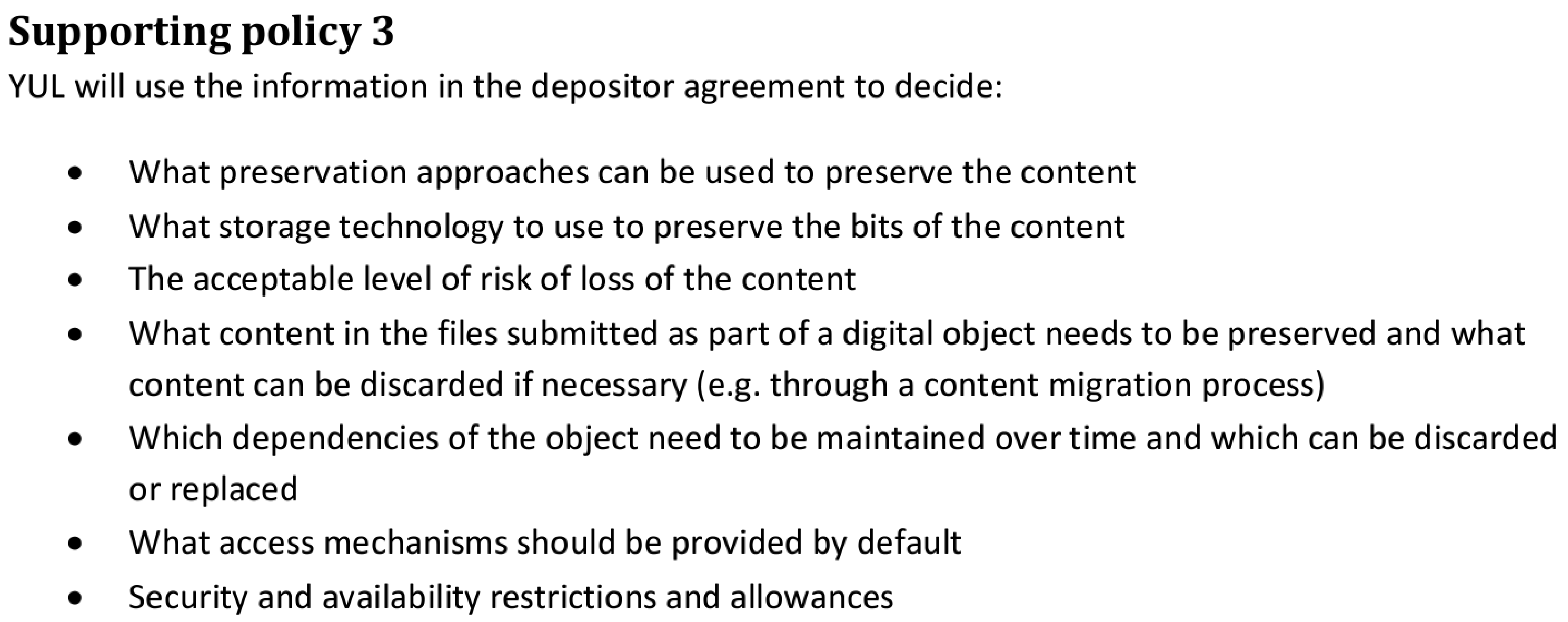
**Where does an institution articulate the goals and commitments that guide its digital preservation work?**

**How might use of the tools and technologies you see in today’s recordings be supported and informed by digital preservation policy?**

# What is digital preservation policy?

“A digital preservation policy expresses a set of principles which will guide an organization in the way it approaches preservation activities and responsibilities. […] The purpose of a policy is to support consistent decision making about digital preservation over time.”

# Digital forensics in policy across the LAM lifecycle: Acquisition

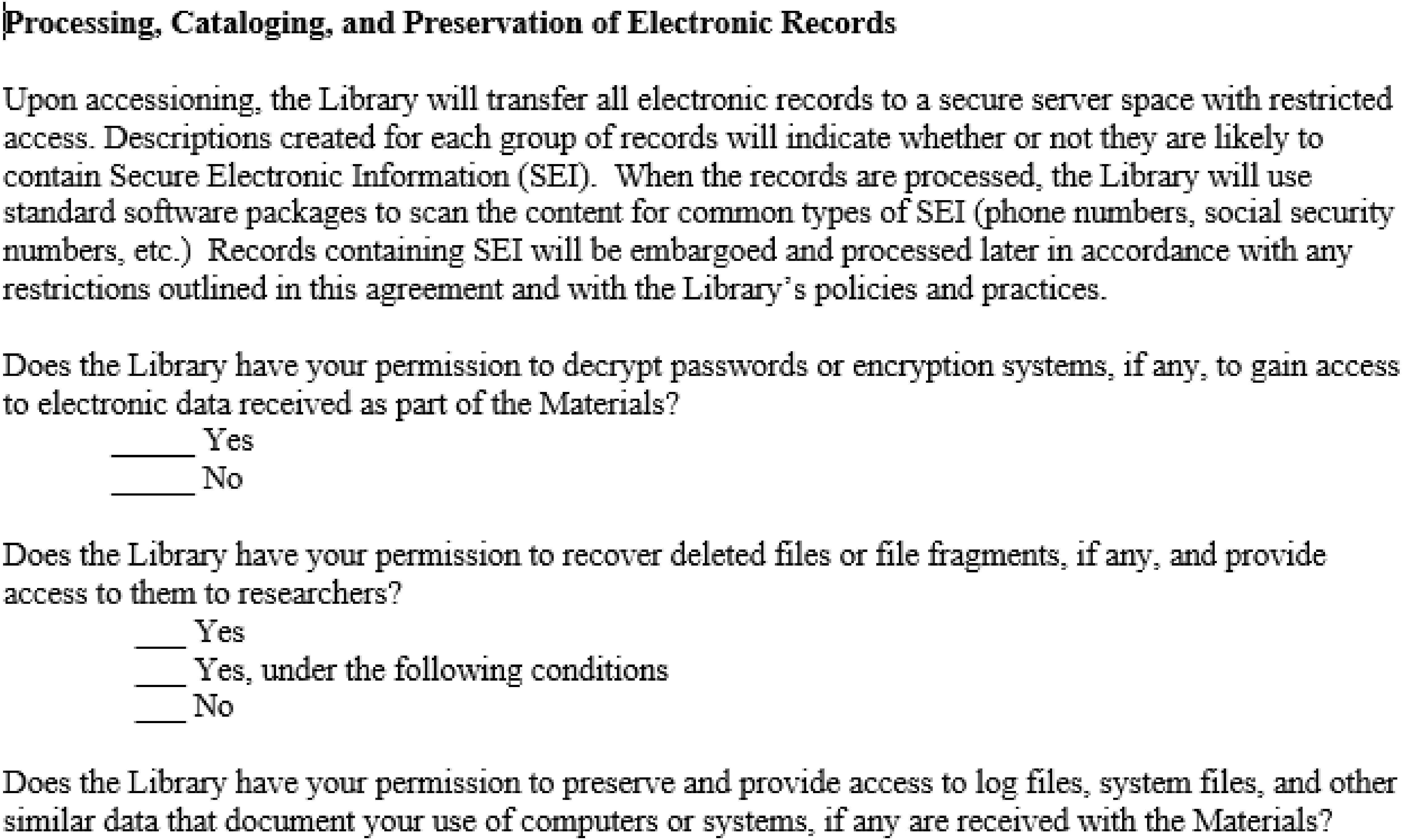


## Supporting policy 3

YUL will use the information in the depositor agreement to decide:

- What preservation approaches can be used to preserve the content
- What storage technology to use to preserve the bits of the content
- The acceptable level of risk of loss of the content
- What content in the files submitted as part of a digital object needs to be preserved and what content can be discarded if necessary (e.g. through a content migration process)
- Which dependencies of the object need to be maintained over time and which can be discarded or replaced
- What access mechanisms should be provided by default
- Security and availability restrictions and allowances

Yale University Libraries Digital Preservation Framework, 2019 https://guides.library.yale.edu/ld.php?content_id=26251943



**Processing, Cataloging, and Preservation of Electronic Records**

Upon accessioning, the Library will transfer all electronic records to a secure server space with restricted access. Descriptions created for each group of records will indicate whether or not they are likely to contain Secure Electronic Information (SEI). When the records are processed, the Library will use standard software packages to scan the content for common types of SEI (phone numbers, social security numbers, etc.) Records containing SEI will be embargoed and processed later in accordance with any restrictions outlined in this agreement and with the Library's policies and practices.

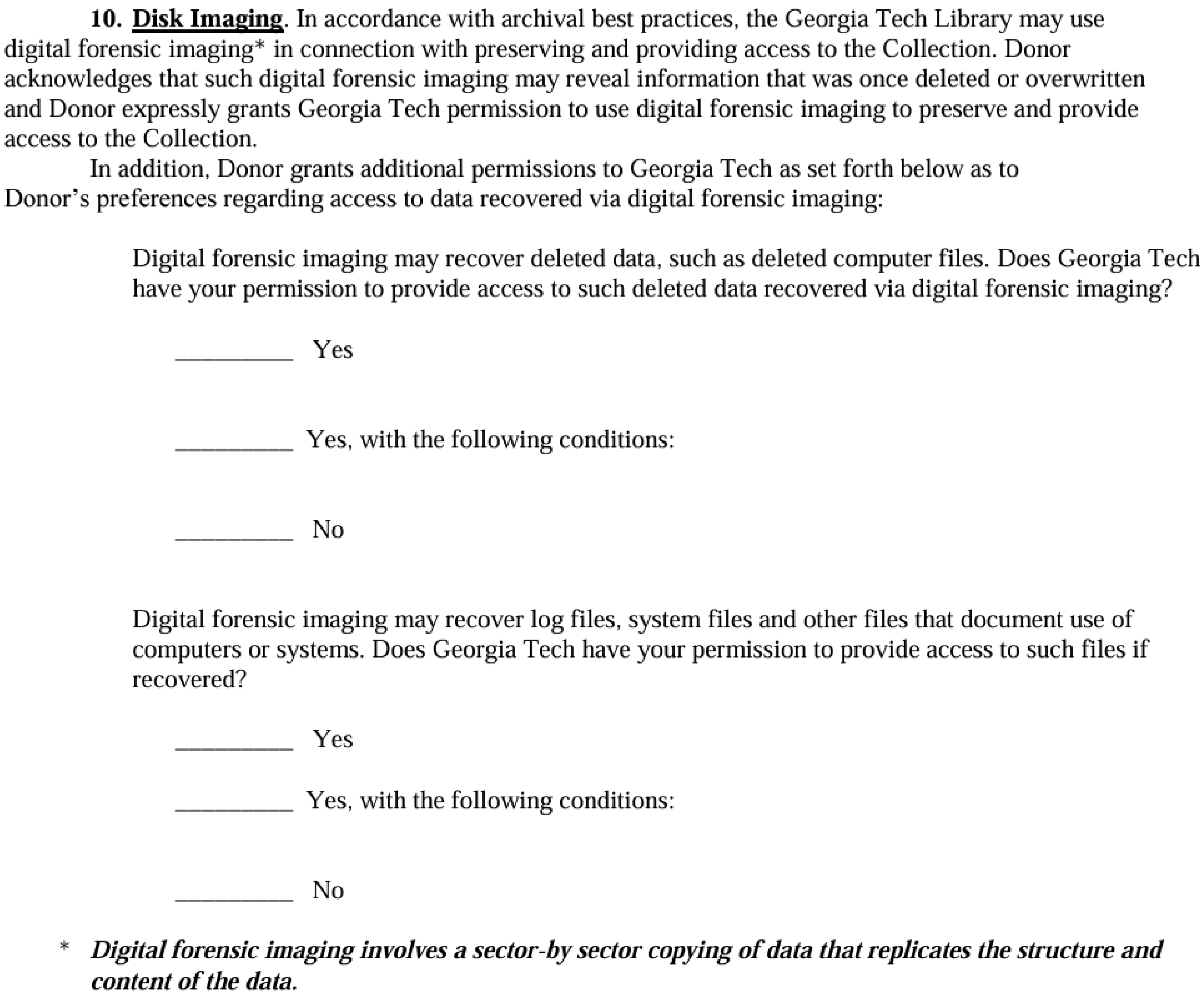
Does the Library have your permission to decrypt passwords or encryption systems, if any, to gain access to electronic data received as part of the Materials?

______ Yes
______ No

Does the Library have your permission to recover deleted files or file fragments, if any, and provide access to them to researchers?

___ Yes
___ Yes, under the following conditions
___ No

Does the Library have your permission to preserve and provide access to log files, system files, and other similar data that document your use of computers or systems, if any are received with the Materials?



**10. Disk Imaging**. In accordance with archival best practices, the Georgia Tech Library may use digital forensic imaging* in connection with preserving and providing access to the Collection. Donor acknowledges that such digital forensic imaging may reveal information that was once deleted or overwritten and Donor expressly grants Georgia Tech permission to use digital forensic imaging to preserve and provide access to the Collection.

In addition, Donor grants additional permissions to Georgia Tech as set forth below as to Donor's preferences regarding access to data recovered via digital forensic imaging:

Digital forensic imaging may recover deleted data, such as deleted computer files. Does Georgia Tech have your permission to provide access to such deleted data recovered via digital forensic imaging?

_________ Yes

_________ Yes, with the following conditions:

_________ No

Digital forensic imaging may recover log files, system files and other files that document use of computers or systems. Does Georgia Tech have your permission to provide access to such files if recovered?

_________ Yes

_________ Yes, with the following conditions:

_________ No

* ***Digital forensic imaging involves a sector-by sector copying of data that replicates the structure and content of the data.***

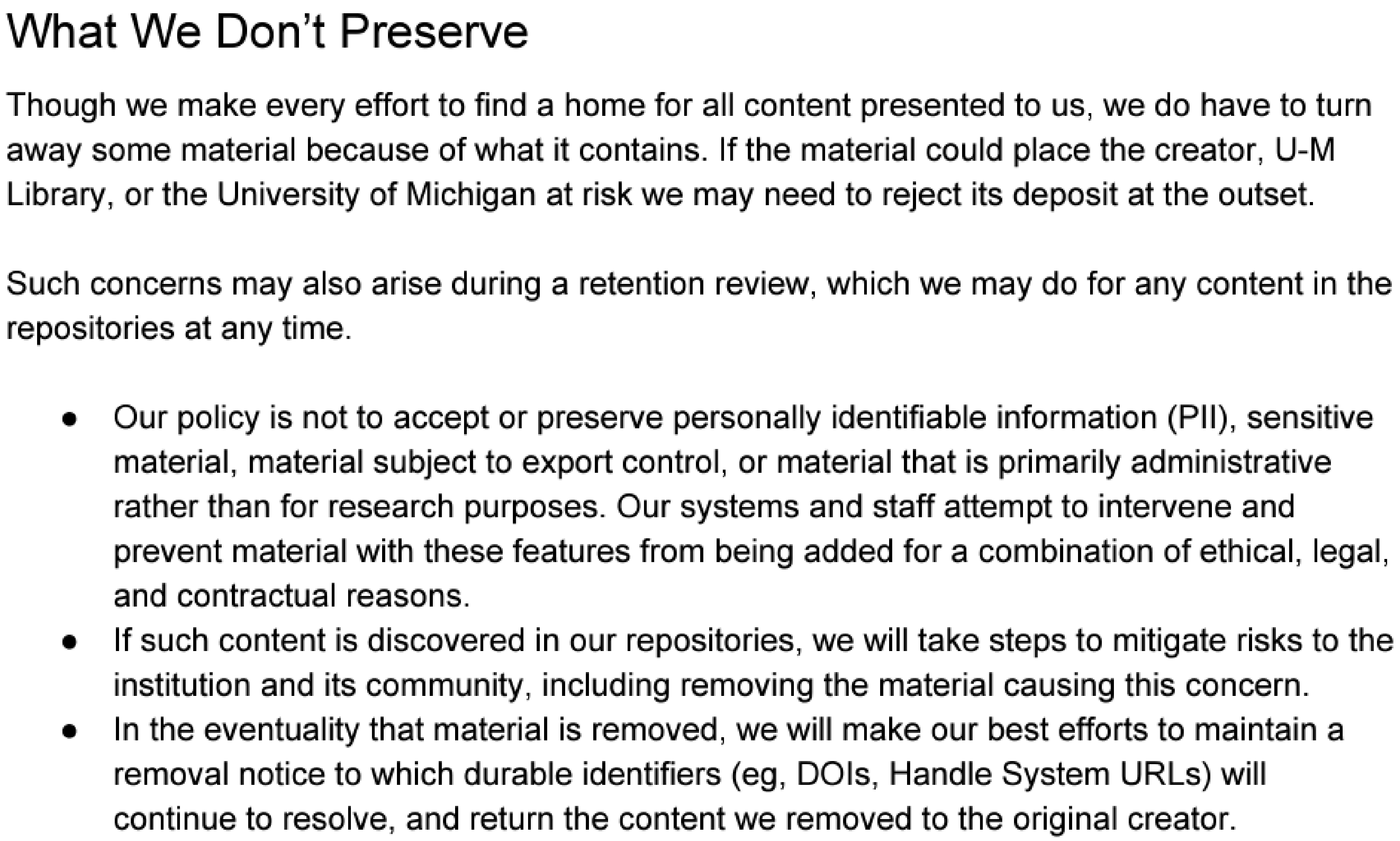
Georgia Tech University, Collection Donation Agreement,
https://library.gatech.edu/sites/default/files/2019-06/Deed-of-Gift-revised.pdf

# Disk Images and DANNNG

- Digital Archival traNsfer, iNgest, and packagiNg Group
- Purpose of Disk Imaging Decision Factors is to demystify disk imaging and the decisions that factor into format selection, creation, handling, and retention.
- Provides detailed technical information to support decision-making around if and when to create a disk image of a storage environment.

https://dannng.github.io/

# Digital forensics in policy across the LAM lifecycle: Processing



## What We Don’t Preserve

Though we make every effort to find a home for all content presented to us, we do have to turn away some material because of what it contains. If the material could place the creator, U-M Library, or the University of Michigan at risk we may need to reject its deposit at the outset.

Such concerns may also arise during a retention review, which we may do for any content in the repositories at any time.

- Our policy is not to accept or preserve personally identifiable information (PII), sensitive material, material subject to export control, or material that is primarily administrative rather than for research purposes. Our systems and staff attempt to intervene and prevent material with these features from being added for a combination of ethical, legal, and contractual reasons.
- If such content is discovered in our repositories, we will take steps to mitigate risks to the institution and its community, including removing the material causing this concern.
- In the eventuality that material is removed, we will make our best efforts to maintain a removal notice to which durable identifiers (eg, DOIs, Handle System URLs) will continue to resolve, and return the content we removed to the original creator.

U-M Library Digital Repository Services Digital Preservation Policy, 2020:
https://www.lib.umich.edu/about-us/policies/digital-repository-services-digital-preservation-policy/

# Disk images and the protection of privacy

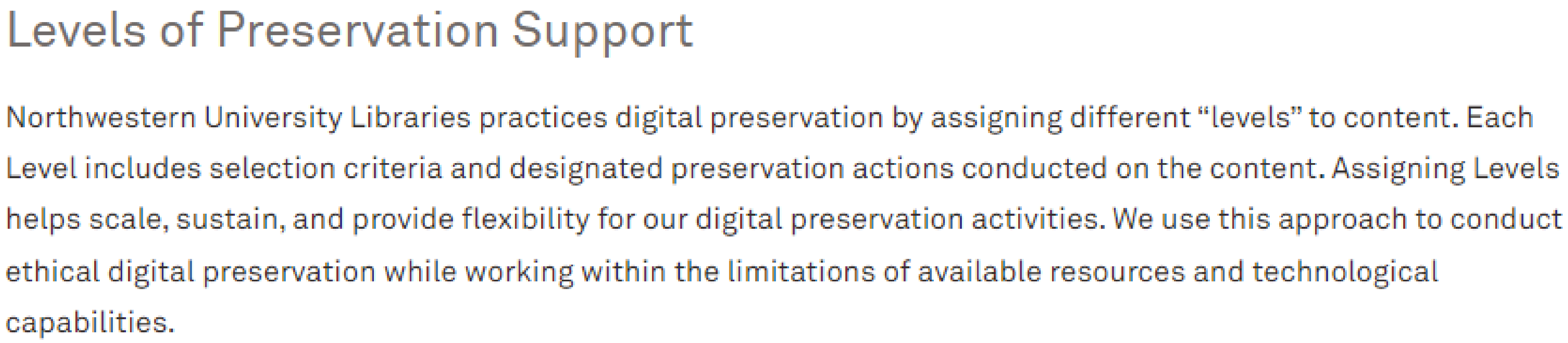
“Balancing Care and Authenticity in Digital Collections: A Radical Empathy Approach to working with Disk Images”
(Lassere and Whyte, 2021)

https://journals.litwinbooks.com/index.php/jclis/article/view/125/102

- Analysis of disk images is resource intensive; keeping disk images by default introduces risk
- Limited tools to mitigate this risk at scale; increases risk and likelihood of harm to people and communities whose materials are collected.

# Digital forensics in policy across the LAM lifecycle: Preservation

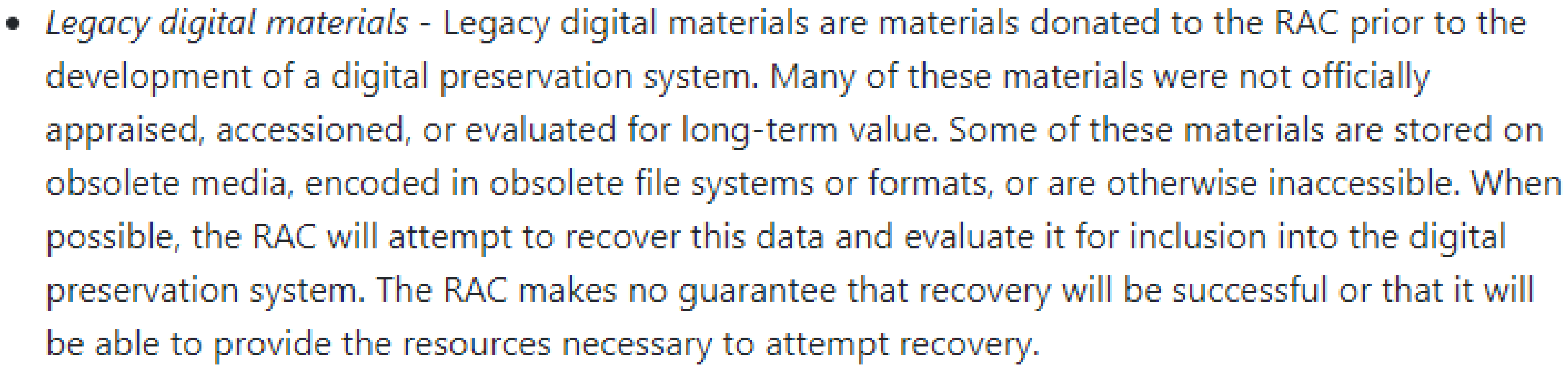
Te Puna Mātauranga o Aotearoa
NATIONAL LIBRARY
OF NEW ZEALAND



## Levels of Preservation Support

Northwestern University Libraries practices digital preservation by assigning different “levels” to content. Each Level includes selection criteria and designated preservation actions conducted on the content. Assigning Levels helps scale, sustain, and provide flexibility for our digital preservation activities. We use this approach to conduct ethical digital preservation while working within the limitations of available resources and technological capabilities.

Northwestern University Libraries Digital Preservation Policy (2023): [https://www.library.northwestern.edu/about/administration/policies/digital-preservation-policy.html](https://www.library.northwestern.edu/about/administration/policies/digital-preservation-policy.html)

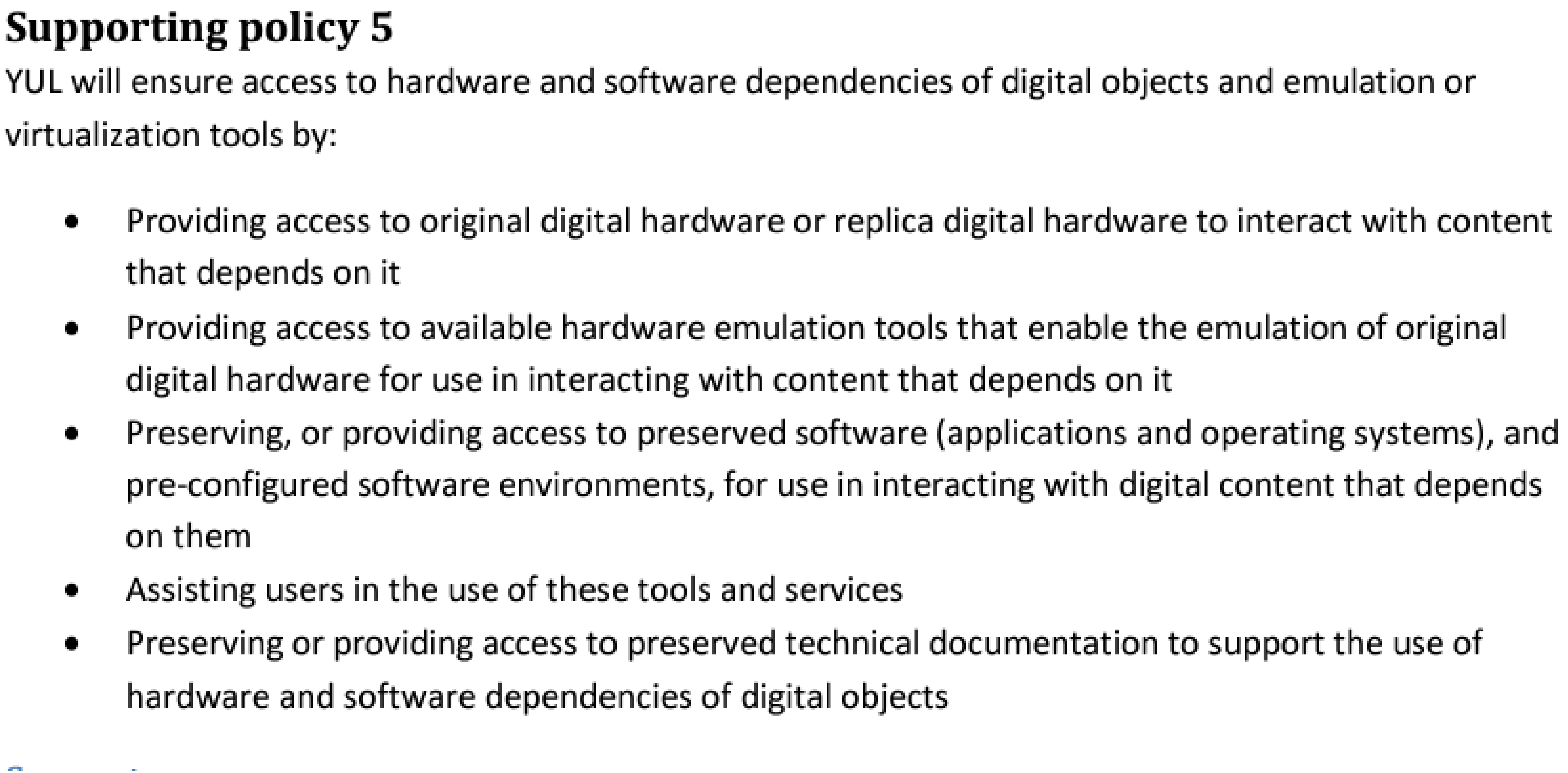


- *Legacy digital materials* - Legacy digital materials are materials donated to the RAC prior to the development of a digital preservation system. Many of these materials were not officially appraised, accessioned, or evaluated for long-term value. Some of these materials are stored on obsolete media, encoded in obsolete file systems or formats, or are otherwise inaccessible. When possible, the RAC will attempt to recover this data and evaluate it for inclusion into the digital preservation system. The RAC makes no guarantee that recovery will be successful or that it will be able to provide the resources necessary to attempt recovery.

Rockefeller Archive Center, Digital Preservation Policy:
https://docs.rockarch.org/digital-preservation-policy#categories-of-commitment

# Digital forensics in policy across the LAM lifecycle: Access

Te Puna Mātauranga o Aotearoa
NATIONAL LIBRARY
OF NEW ZEALAND



## Supporting policy 5

YUL will ensure access to hardware and software dependencies of digital objects and emulation or virtualization tools by:

- Providing access to original digital hardware or replica digital hardware to interact with content that depends on it
- Providing access to available hardware emulation tools that enable the emulation of original digital hardware for use in interacting with content that depends on it
- Preserving, or providing access to preserved software (applications and operating systems), and pre-configured software environments, for use in interacting with digital content that depends on them
- Assisting users in the use of these tools and services
- Preserving or providing access to preserved technical documentation to support the use of hardware and software dependencies of digital objects

Yale University Libraries Digital Preservation Framework, 2019 https://guides.library.yale.edu/ld.php?content_id=26251943

# Conclusions

- Digital forensics tools and processes have provided LAM institutions with **new ways to interact with digital information.**
- The fields of digital forensics and digital preservation are aligned in their emphasis on maintaining the integrity and authenticity of digital information but have important differences in **intent**.
- The opportunities afforded by **implementing** digital forensics tools and processes can be **complemented** by digital preservation policy statements that support decision-making around the use of those tools and processes.

# Thank you!