Selected Excerpts from the TCPS2 2014

Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada, Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, December 2014.

Note: For the most recent information on amendments, please consult the official online version of the TCPS at *www.pre.ethics.gc.ca*.

Ethics Framework: [Chapter 1, page 5]
Research is a step into the unknown. Because it seeks to understand something not yet revealed, research often entails risks to participants and others. These risks can be trivial or profound, physical or psychological, individual or social. History offers unfortunate examples where research participants have been needlessly, and at times profoundly, harmed by research, sometimes even dying as a result. Ethical principles and guidelines play an important role in advancing the pursuit of knowledge while protecting and respecting research participants in order to try to prevent such occurrences.

People have also been gratified and have had their lives enriched by their participation in research, either because they may have benefited directly or because their participation has contributed to the expansion of knowledge. Given the fundamental importance of research and of human participation in research, we must do all that we can as a society to ensure that research is conducted in an ethical manner so as to build public confidence and trust. By promoting and guiding the ethical conduct of research involving humans, this Policy seeks to contribute tangibly to these goals.

Core Principles: [Chapter 1, page 6]
Respect for human dignity requires that research involving humans be conducted in a manner that is sensitive to the inherent worth of all human beings and the respect and consideration that they are due. In this Policy, respect for human dignity is expressed through three core principles – Respect for Persons, Concern for Welfare, and Justice. These core principles transcend disciplinary boundaries and, therefore, are relevant to the full range of research covered by this Policy.1

[Chapter 1, page 6]
An important mechanism for respecting participants' autonomy in research is the requirement to seek their free, informed and ongoing consent. This requirement reflects the commitment that participation in research, including participation through the use of one's data or biological materials, should be a matter of choice and that, to be meaningful, the choice must be informed. An informed choice is one that is based on as complete an understanding as is reasonably possible of the purpose of the research, what it entails, and its foreseeable risks and potential benefits, both to the participant and to others. Respect for Persons also includes a commitment to accountability and transparency in the ethical conduct of research.

Research Ethics and Law [Chapter 1, page 10]
In addition to the principles and guidelines in this Policy, researchers are responsible for ascertaining and complying with all applicable legal and regulatory requirements with respect to consent and the protection of privacy of participants (see Chapter 5). These legal and regulatory requirements may vary depending on the jurisdiction in Canada in which the

research is being conducted, and who is funding and/or conducting the research, and they may comprise constitutional, statutory, regulatory, common law, and/or international or legal requirements of jurisdictions outside of Canada. Where the research is considered to be a governmental activity, for example, standards for protecting privacy flowing from the *Canadian Charter of Rights and Freedoms*, federal privacy legislation and regulatory requirements would apply.

Privacy and Confidentiality: [Chapter 5 excerpts from TCPS2 pages 57 - 64, please go to see the online .pdf of the TCPS2 for the complete Application of each Article]

…respect for privacy in research is an internationally recognized norm and ethical standard.

Privacy risks in research relate to the identifiability of participants, and the potential harms they, or groups to which they belong, may experience from the collection, use and disclosure of personal information. Privacy risks arise at all stages of the research life cycle, including initial collection of information, use and analysis to address research questions, dissemination of findings, storage and retention of information, and disposal of records or devices on which information is stored.

The assessment of whether information is identifiable is made in the context of a specific research project.

Ethical concerns regarding privacy decrease as it becomes more difficult (or impossible) to associate information with a particular individual. These concerns also vary with the sensitivity of the information and the extent to which access, use or disclosure may harm an individual or group.

Technological developments have increased the ability to access, store and analyze large volumes of data. These activities may heighten risks of re-identification, such as when researchers link datasets (see Section E, this chapter), or where a dataset contains information about a population in a small geographical area, or about individuals with unique characteristics (e.g., uncommon field of occupational specialization, diagnosis of a very rare disease). Various factors can affect the risks of re-identification, and researchers and REBs should be vigilant in their efforts to recognize and reduce these risks. Data linkage of two or more datasets of anonymous information may present risks of identification (see Article 2.4 or Article 9.22).

Article 5.1 Researchers shall safeguard information entrusted to them and not misuse or wrongfully disclose it. Institutions shall support their researchers in maintaining promises of confidentiality.

Article 5.2 Researchers shall describe measures for meeting confidentiality obligations and explain any reasonably foreseeable disclosure requirements:
(a) in application materials they submit to the REB; and
(b) during the consent process with prospective participants.

Article 5.3 Researchers shall provide details to the REB regarding their proposed measures for safeguarding information, for the full life cycle of information: its collection, use, dissemination, retention and/or disposal.

Article 5.4 Institutions or organizations where research data are held have a responsibility to establish appropriate institutional security safeguards.
Application In addition to the security measures researchers implement to protect data, safeguards put in place at the institutional or organizational level also provide important protection. These data security

Note: For the most recent information on amendments, please consult the official online version of the TCPS at *www.pre.ethics.gc.ca*.

safeguards should include adequate physical, administrative and technical measures, and should address the full life cycle of information. This includes institutional or organizational safeguards for information while it is currently in use by researchers, and for any long-term retention of information.

What is Research as defined in the TCPS2:

A. Scope of Research Ethics Review [Chapter 2 found on pages 13 & 14]

Research Requiring REB Review

The following article defines the general categories of research that require REB review in accordance with this Policy, subject to the exceptions set out further on in this Policy. These exceptions are distinct from research that is exempt from REB review, as described in Articles 2.2 to 2.4.

Article 2.1 The following requires ethics review and approval by an REB before the research commences:

(a) research involving living human participants;

(b) research involving human biological materials, as well as human embryos, fetuses, fetal tissue, reproductive materials and stem cells. This applies to materials derived from living and deceased individuals.

Application The scope of this Policy is restricted to the review of the ethical conduct of research involving humans. The scope of REB review is limited to those activities defined in this Policy as "research" involving "human participants."

For the purposes of this Policy, "research" is defined as an undertaking intended to extend knowledge through a disciplined inquiry and/or systematic investigation. The term "disciplined inquiry" refers to an inquiry that is conducted with the expectation that the method, results, and conclusions will be able to withstand the scrutiny of the relevant research community. For example, a study seeking to explore the narratives of teens coping with mental illness would be evaluated by the established standards of studies employing similar methods, technologies and/or theoretical frameworks.

A determination that research is the intended purpose of the undertaking is key for differentiating activities that require ethics review by an REB and those that do not (see Article 2.5). In some cases it can be difficult to make this distinction, underscoring the need to have reviewers or ad hoc advisors (see Articles 6.4 and 6.5) who can assist with this determination. It is important to note that choice of methodology and/or intent or ability to publish findings are not factors that determine whether or not an activity is research requiring ethics review.

For the purposes of this Policy, "human participants" (referred to as "participants") are those individuals whose data, or responses to interventions, stimuli or questions by the researcher, are relevant to answering the research question.

Research Exempt from REB Review [Chapter 2 found on pages 15 through 19, **only the Articles are included here, please go to see the online .pdf for the complete Application of each Article**]

Some research is exempt from REB review where protections are available by other means. This Policy allows the following exemptions from the requirement for REB review, as outlined below.

Article 2.2 Research that relies exclusively on publicly available information does not require REB review when:
(a) the information is legally accessible to the public and appropriately protected by law; or
(b) the information is publicly accessible and there is no reasonable expectation of privacy.

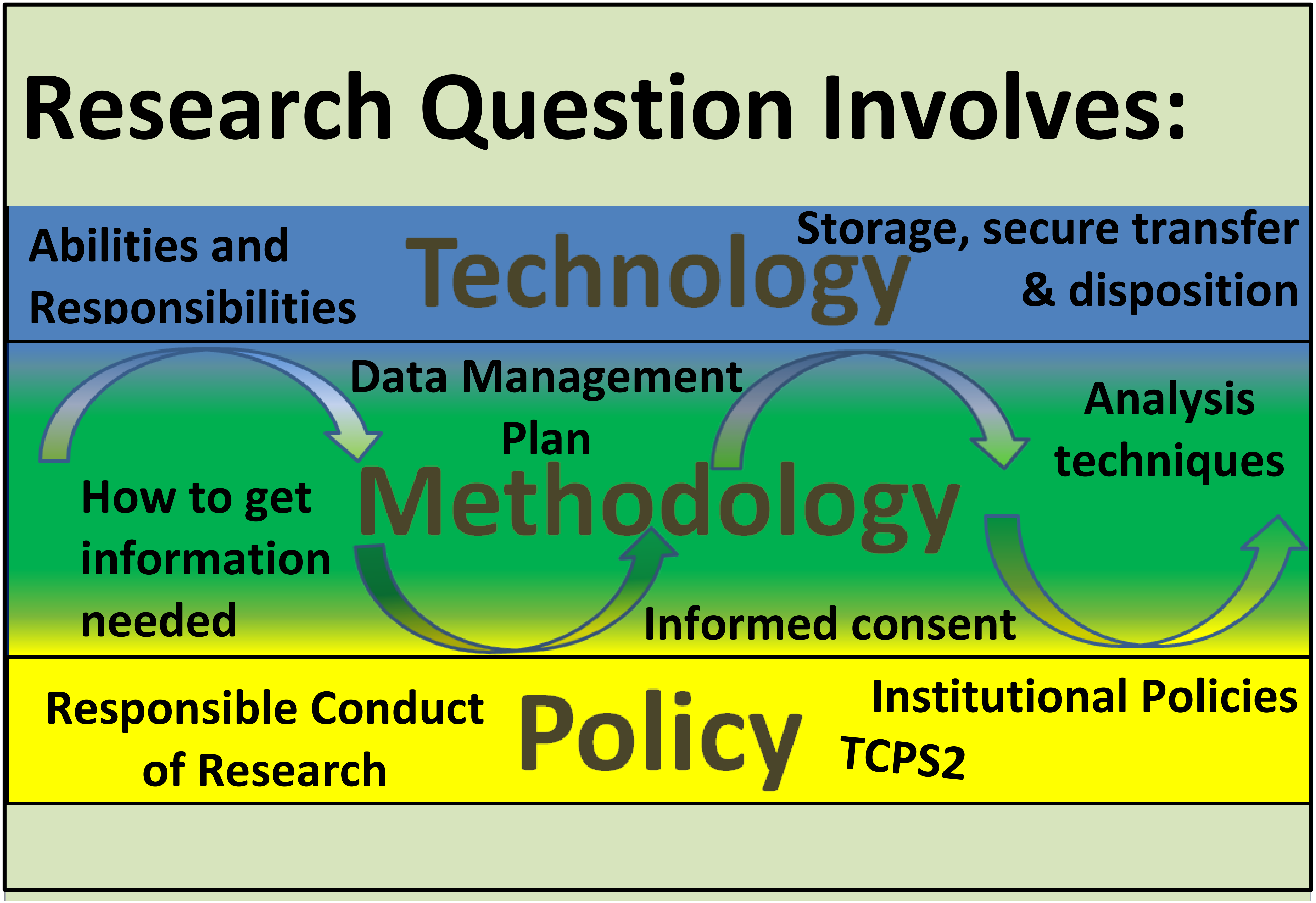
Article 2.3 REB review is not required for research involving the observation of people in public places where:
(a) it does not involve any intervention staged by the researcher, or direct interaction with the individuals or groups;
(b) individuals or groups targeted for observation have no reasonable expectation of privacy; and
(c) any dissemination of research results does not allow identification of specific individuals.

Article 2.4 REB review is not required for research that relies exclusively on secondary use of anonymous information, or anonymous human biological materials, so long as the process of data linkage or recording or dissemination of results does not generate identifiable information.

Activities Not Requiring REB Review
The following distinguishes research requiring REB review from non-research activities that have traditionally employed methods and techniques similar to those employed in research. Such activities are not considered "research" as defined in this Policy, and do not require REB review.
Activities outside the scope of research subject to REB review (see Articles 2.5 and 2.6), as defined in this Policy, may still raise ethical issues that would benefit from careful consideration by an individual or a body capable of providing some independent guidance, other than an REB. These ethics resources may be based in professional or disciplinary associations, particularly where those associations have established best practices guidelines for such activities in their discipline.

Article 2.5 Quality assurance and quality improvement studies, program evaluation activities, and performance reviews, or testing within normal educational requirements when used exclusively for assessment, management or improvement purposes, do not constitute research for the purposes of this Policy, and do not fall within the scope of REB review.

Article 2.6 Creative practice activities, in and of themselves, do not require REB review. However, research that employs creative practice to obtain responses from participants that will be analyzed to answer a research question is subject to REB review.



Research Question Involves:

Abilities and Responsibilities

Technology

Storage, secure transfer & disposition

Data Management Plan

Analysis techniques

How to get information needed

Methodology

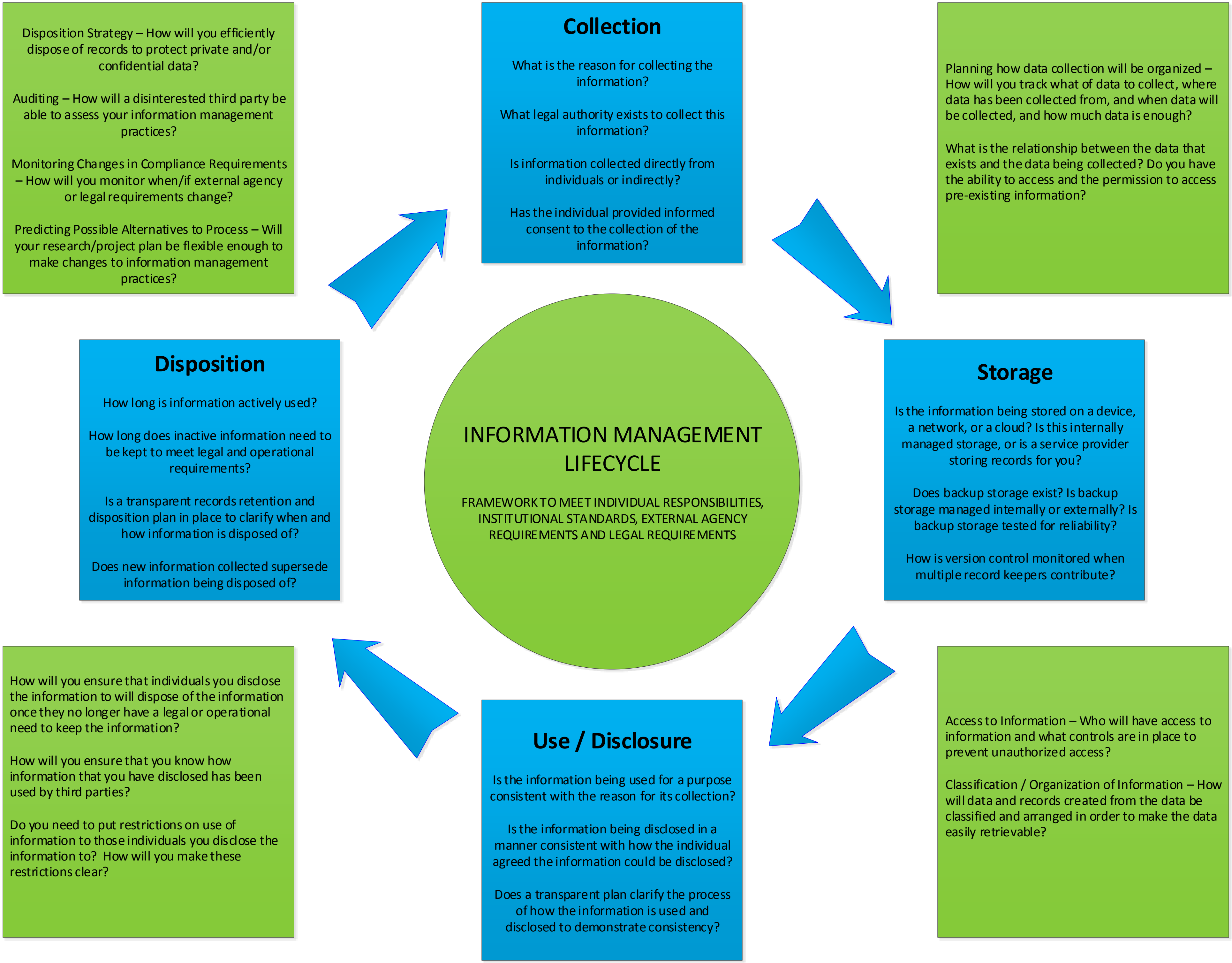
Informed consent

Responsible Conduct of Research

Policy

Institutional Policies

TCPS2



INFORMATION MANAGEMENT LIFECYCLE

FRAMEWORK TO MEET INDIVIDUAL RESPONSIBILITIES, INSTITUTIONAL STANDARDS, EXTERNAL AGENCY REQUIREMENTS AND LEGAL REQUIREMENTS

Collection

What is the reason for collecting the information?

What legal authority exists to collect this information?

Is information collected directly from individuals or indirectly?

Has the individual provided informed consent to the collection of the information?

Planning how data collection will be organized – How will you track what of data to collect, where data has been collected from, and when data will be collected, and how much data is enough?

What is the relationship between the data that exists and the data being collected? Do you have the ability to access and the permission to access pre-existing information?

Storage

Is the information being stored on a device, a network, or a cloud? Is this internally managed storage, or is a service provider storing records for you?

Does backup storage exist? Is backup storage managed internally or externally? Is backup storage tested for reliability?

How is version control monitored when multiple record keepers contribute?

Access to Information – Who will have access to information and what controls are in place to prevent unauthorized access?

Classification / Organization of Information – How will data and records created from the data be classified and arranged in order to make the data easily retrievable?

Use / Disclosure

Is the information being used for a purpose consistent with the reason for its collection?

Is the information being disclosed in a manner consistent with how the individual agreed the information could be disclosed?

Does a transparent plan clarify the process of how the information is used and disclosed to demonstrate consistency?

How will you ensure that individuals you disclose the information to will dispose of the information once they no longer have a legal or operational need to keep the information?

How will you ensure that you know how information that you have disclosed has been used by third parties?

Do you need to put restrictions on use of information to those individuals you disclose the information to? How will you make these restrictions clear?

Disposition

How long is information actively used?

How long does inactive information need to be kept to meet legal and operational requirements?

Is a transparent records retention and disposition plan in place to clarify when and how information is disposed of?

Does new information collected supersede information being disposed of?

Disposition Strategy – How will you efficiently dispose of records to protect private and/or confidential data?

Auditing – How will a disinterested third party be able to assess your information management practices?

Monitoring Changes in Compliance Requirements – How will you monitor when/if external agency or legal requirements change?

Predicting Possible Alternatives to Process – Will your research/project plan be flexible enough to make changes to information management practices?

Categories of Risk for Breach of Personal Privacy

	Restricted	Sensitive	Internal	Public
Definition	Information that the institution is legally responsible for protecting and/or information that could be used to cause identity theft of individuals in the university community if unintentionally or maliciously released.	Factual information or draft records that can reasonably be expected to cause harm to an individual or the organization if the information is unintentionally or maliciously released.	Factual information, advice, recommendations or drafts of records that may be damaging to the institution or an individual if that information is released before being assessed and severed.	Factual information made available to the public or information that can be released to the public if requested without needing to be assessed and severed.
Examples	Criminal Record/Credit Check Information, Identity Records (information from: driver's license, BC ID, BC Services Card, SINs, Passports, Study/Work Permits, Temporary Resident Visas, Completed Legal Change of Name Forms)	Personnel Records, Official Employee Evaluations, Individual Demographic Information, Personal Contact Information, Student/Employee IDs, Employment Relations Records,	Meeting notes of informal meetings, records highlighting unofficial recommendations, personal opinions or character references about individuals, employment groups or departments at UNBC, planning documentation, personal correspondence, any drafts of records found in the public category, small pool statistics	Business contact information, promotional materials, information posted on UNBC's public websites, syllabi, active institutional policies and procedures, job descriptions, job postings, position pay grades, minutes of public meetings, large pool statistics, published materials such as academic calendars

	Restricted	Sensitive	Internal	Public
Impact of Unintentional or Malicious Release	The individual could suffer major harm including identity theft. The institution and/or employees could be financially responsible for covering substantive damages.	The individual may suffer loss of opportunity, embarrassment, or financial harm. The individual may be harassed as a result of the release of this information. UNBC or members of the UNBC community will suffer reputational damage and details of leaked information may appear in newspapers and other media. The institution may be responsible for paying for damages.	The public is misinformed about processes or events managed by UNBC or members of the university community or individuals lose confidence with UNBC's and employees of UNBC's ability to handle information. May result in minor reputational or financial damage.	Impacts are minimal and already accounted for when the information is posted or provided to the public.
Recommended Management of Information	Restrict circulation of these records to the minimum number of individuals that require the information to complete their operational duties. Put the information in encrypted documents and databases. Avoid replicating the information unless operationally required. Dispose or aggregate out this category of personal information as soon as operationally possible.	Restrict circulation of these records to individuals that require the information to complete their operational duties. Lock doors, lock cabinets, lock computers and close central repositories holding this information when it is not in use.	Employees need to indicate that records are confidential if the contents of these records cannot be released to the public (i.e. Confidential watermark or confidential indicator in email signatures)	Proactively provide this information to the public in a convenient way.

UNBC

IT SECURITY

What is encryption?

At it’s simplest, encryption is a way to lock your data to protect it from unauthorized access. A key is used to scramble the data and then to restore it when needed.

Why do we need to encrypt data?

To comply with various privacy standards and federal and provincial laws, we have to encrypt data that may allow an outside individual to identify a person based on that data. Protecting your sensitive research materials is another good reason to encrypt your data, especially while travelling. This protects not only your data, it also reduces your liability if your storage device or laptop get lost or stolen.

How do I encrypt my data?

Most UNBC owned laptops and tablets have their hard drives encrypted before they are deployed to their users. If you are not sure if your laptop has been encrypted, contact the Service Desk and they can assist you with getting your drive encrypted.

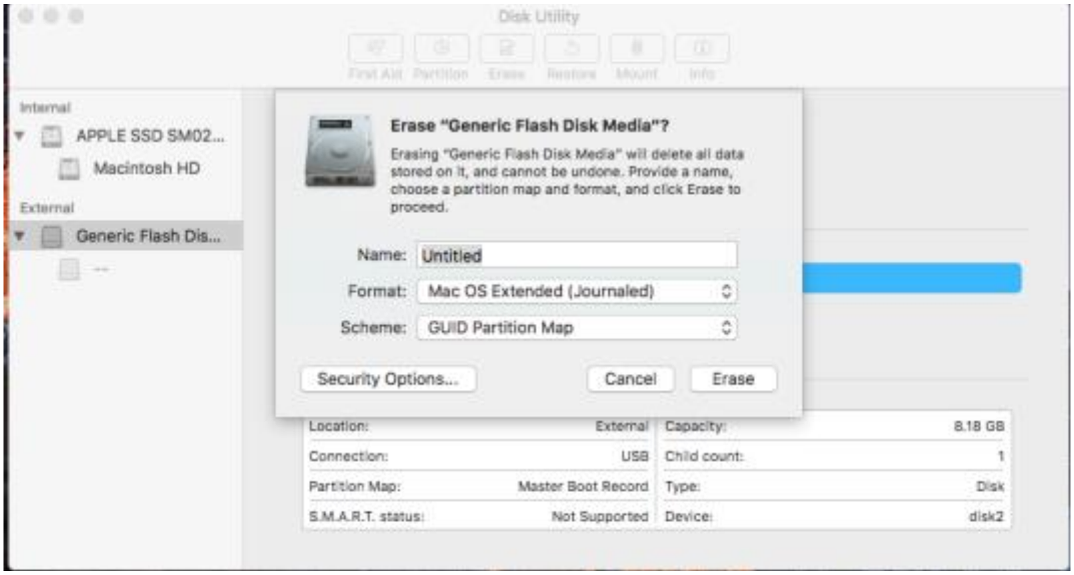
You can also encrypt your portable storage devices. Most popular operating systems will have an encryption product built in. Microsoft uses Bitlocker, Apple uses FileVault. Instructions on their use can be found on the I.T. Security sharepoint site under https://our.unbc.ca. If you require further assistance, you can contact the Service Desk.

To safely and securely share your data with researchers and other authorized users, UNBC recommends using Sync as a file sharing service, and PeaZip to password protect and compress your files. Instructions for these can be found on the I.T. Security sharepoint site as well. The Service Desk can also assist you with Sync and PeaZip.

Encrypting a drive with FileVault

Insert your portable storage device

Go to Finder>Applications>Disk Utility



Erase "Generic Flash Disk Media"?

Erasing "Generic Flash Disk Media" will delete all data stored on it, and cannot be undone. Provide a name, choose a partition map and format, and click Erase to proceed.

Name: Untitled

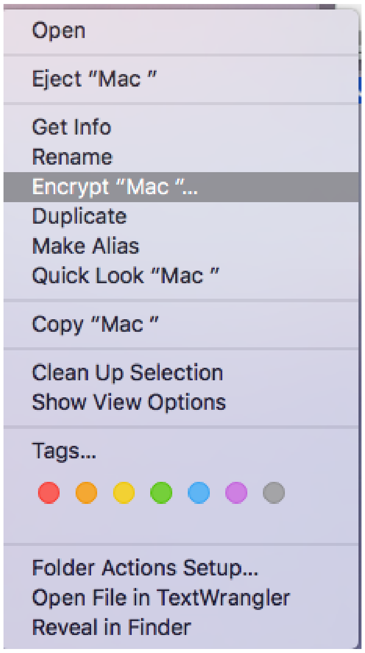
Format: Mac OS Extended (Journaled)

Scheme: GUID Partition Map

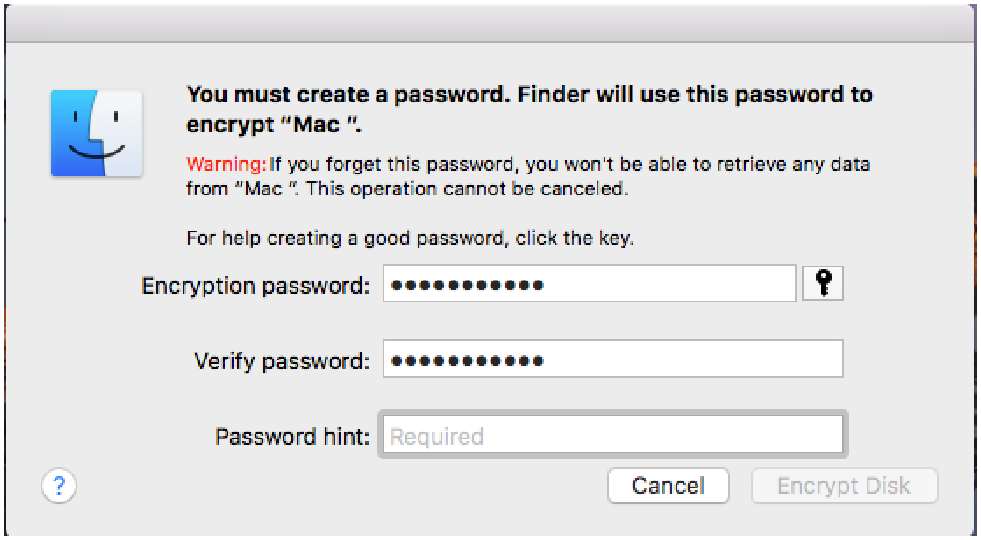
Location:	External	Capacity:	8.18 GB
Connection:	USB	Child count:	1
Partition Map:	Master Boot Record	Type:	Disk
S.M.A.R.T. status:	Not Supported	Device:	disk2

Most portable storage devices are formatted to work with Microsoft Windows. To encrypt a storage device for an Apple device, you'll have to erase it and format it as above.

Once the drive has been erased and formatted properly, right click on the drive



Enter a password that you will use to decrypt the drive and a hint. Click Encrypt Disk



You must create a password. Finder will use this password to encrypt "Mac ".

Warning: If you forget this password, you won't be able to retrieve any data from "Mac ". This operation cannot be canceled.

For help creating a good password, click the key.

Encryption password: ●●●●●●●●●●●●

Verify password: ●●●●●●●●●●●●

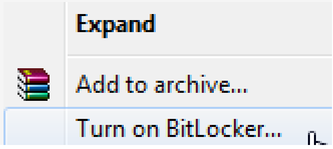
Password hint: Required

Wait for your storage device to be encrypted

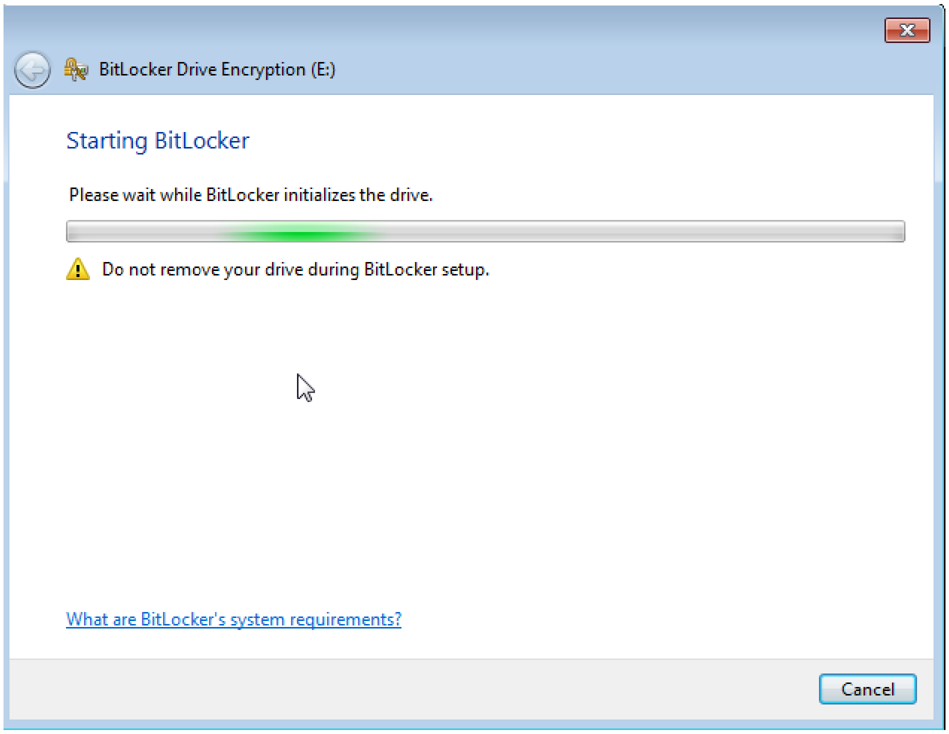
Encrypting portable storage with Bitlocker

Insert your portable storage into your computer

Right click on the drive and select Turn on BitLocker



BitLocker will start, wait until it prompts you



BitLocker Drive Encryption (E:)

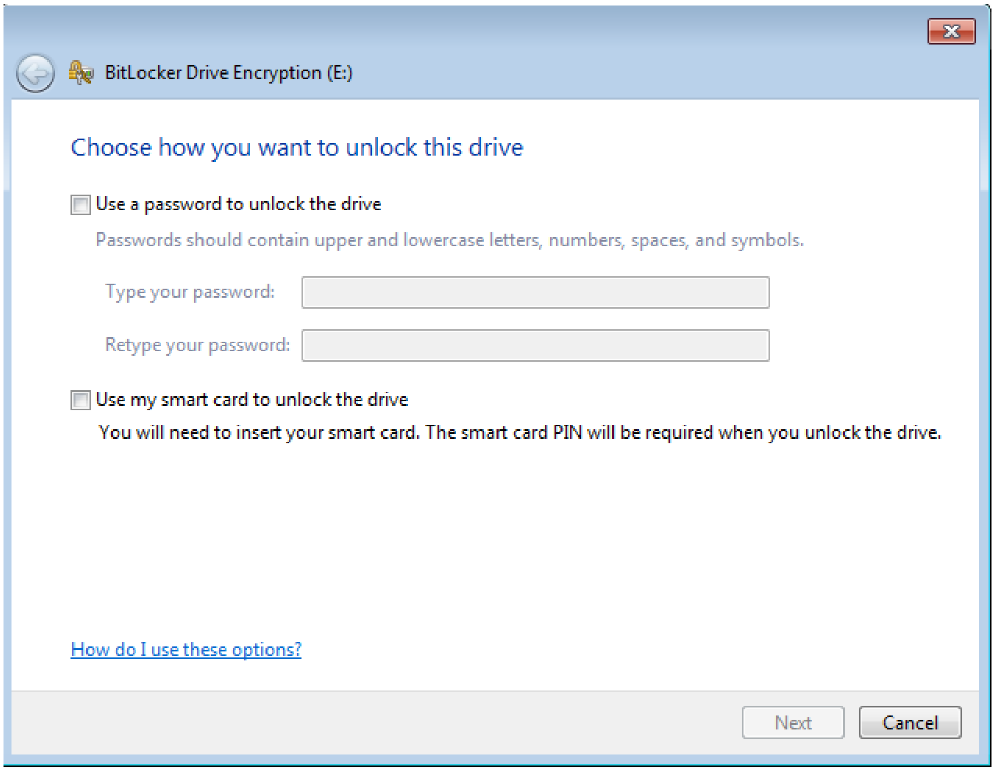
Starting BitLocker

Please wait while BitLocker initializes the drive.

⚠ Do not remove your drive during BitLocker setup.

What are BitLocker's system requirements?

Choose a password that you’ll use to unlock the drive when you want to use it.



Choose how you want to unlock this drive

□ Use a password to unlock the drive

Passwords should contain upper and lowercase letters, numbers, spaces, and symbols.

Type your password:

Retype your password:

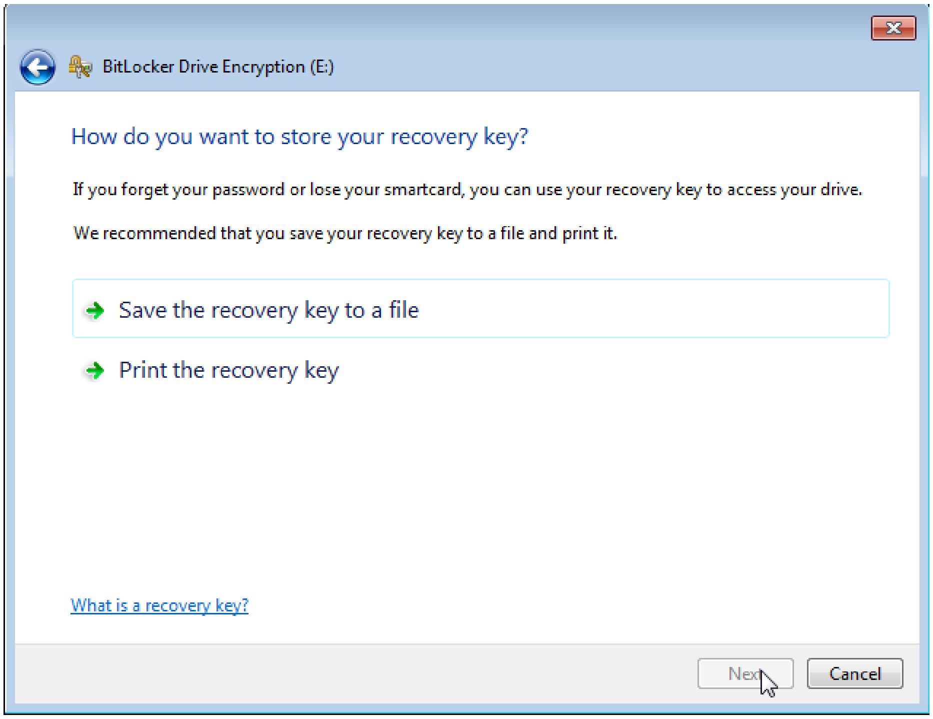
□ Use my smart card to unlock the drive

You will need to insert your smart card. The smart card PIN will be required when you unlock the drive.

How do I use these options?

Save or print the recovery key.

**** The recovery key can be used to unlock the device if you forget the password. Do not lose it!**



How do you want to store your recovery key?

If you forget your password or lose your smartcard, you can use your recovery key to access your drive.

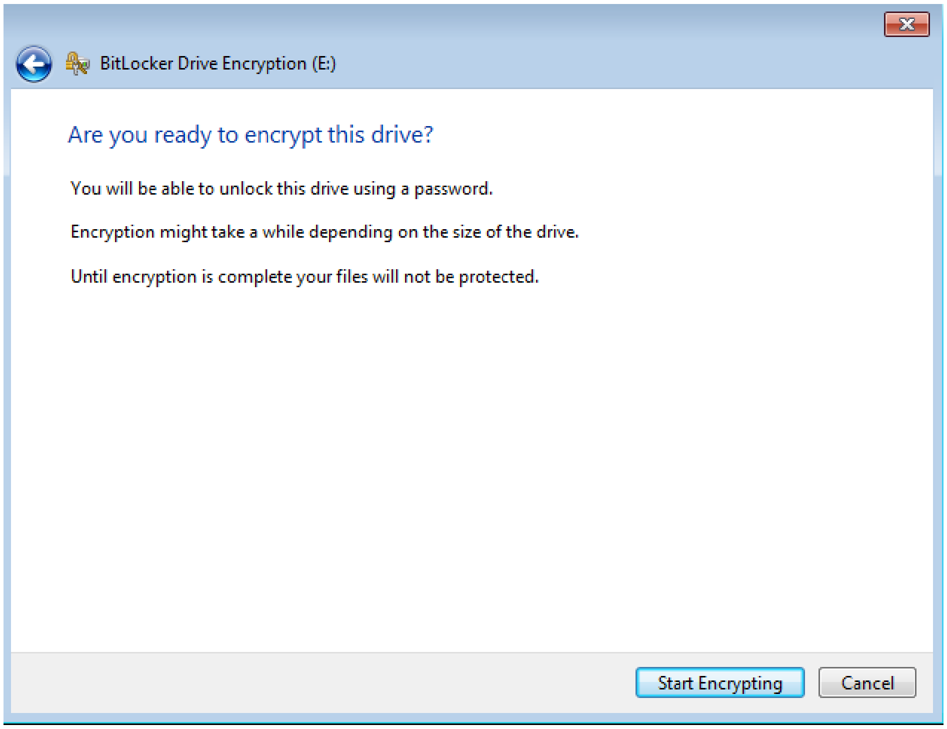
We recommended that you save your recovery key to a file and print it.

→ Save the recovery key to a file

→ Print the recovery key

What is a recovery key?

Select an option and click Next to begin encrypting your drive.



Are you ready to encrypt this drive?

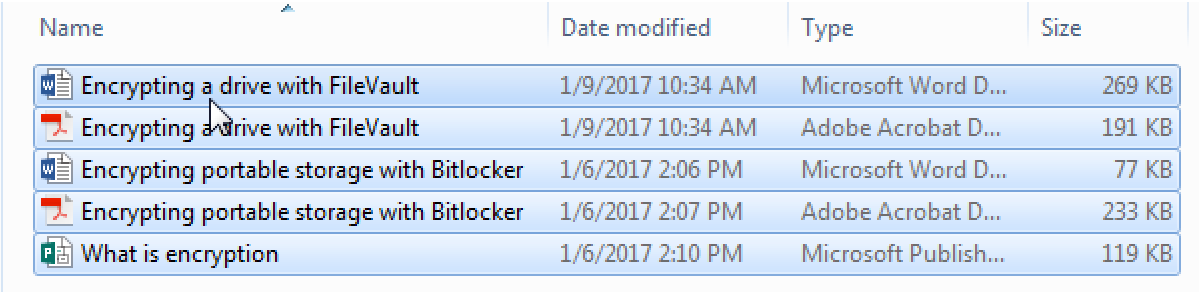
You will be able to unlock this drive using a password.

Encryption might take a while depending on the size of the drive.

Until encryption is complete your files will not be protected.

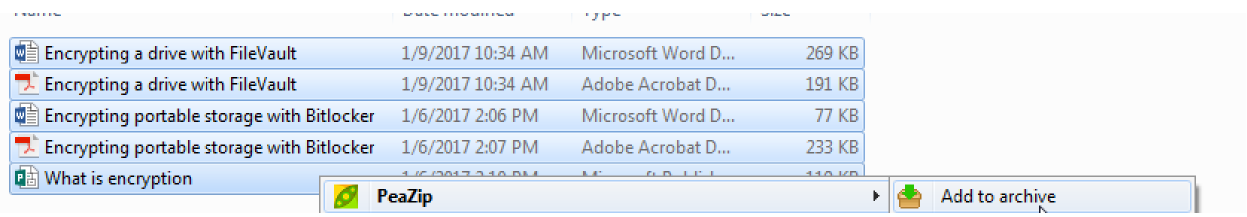
Protecting files with PeaZip

Select the files you wish to zip



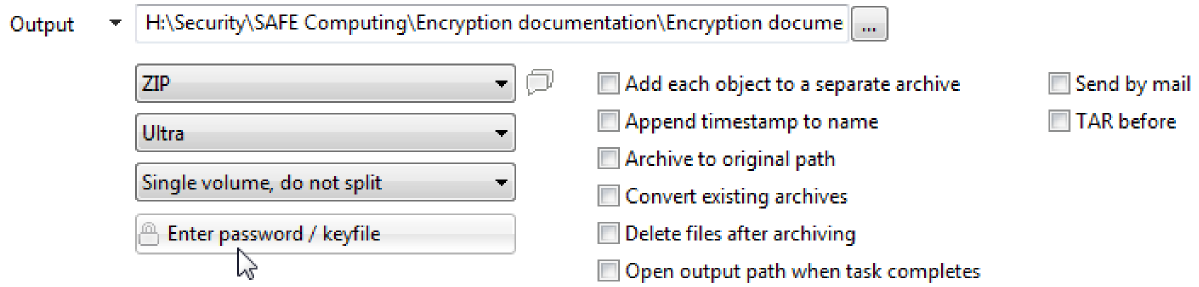
Name	Date modified	Type	Size
Encrypting a drive with FileVault	1/9/2017 10:34 AM	Microsoft Word D...	269 KB
Encrypting a drive with FileVault	1/9/2017 10:34 AM	Adobe Acrobat D...	191 KB
Encrypting portable storage with Bitlocker	1/6/2017 2:06 PM	Microsoft Word D...	77 KB
Encrypting portable storage with Bitlocker	1/6/2017 2:07 PM	Adobe Acrobat D...	233 KB
What is encryption	1/6/2017 2:10 PM	Microsoft Publish...	119 KB

Right click on the files and select PeaZip>Add to Archive



Name	Date modified	Type	Size
Encrypting a drive with FileVault	1/9/2017 10:34 AM	Microsoft Word D...	269 KB
Encrypting a drive with FileVault	1/9/2017 10:34 AM	Adobe Acrobat D...	191 KB
Encrypting portable storage with Bitlocker	1/6/2017 2:06 PM	Microsoft Word D...	77 KB
Encrypting portable storage with Bitlocker	1/6/2017 2:07 PM	Adobe Acrobat D...	233 KB
What is encryption			

At the bottom left of the page, there is a lock icon that allows you to create a password to secure your files



Output H:\Security\SAFE Computing\Encryption documentation\Encryption docume

ZIP

Ultra

Single volume, do not split

Enter password / keyfile

☐ Add each object to a separate archive

☐ Append timestamp to name

☐ Archive to original path

☐ Convert existing archives

☐ Delete files after archiving

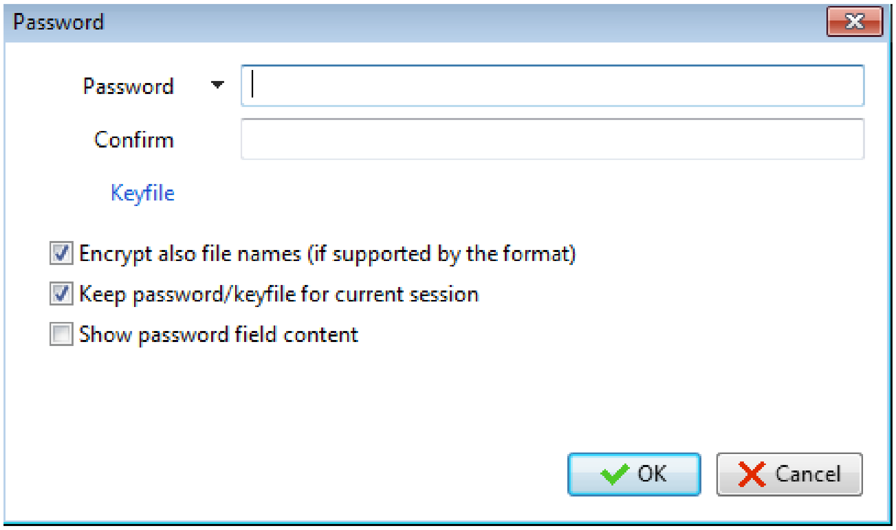
☐ Open output path when task completes

☐ Send by mail

☐ TAR before

Enter a password

<u> Please remember. It is extremely difficult and in some cases impossible to recover an archive that has been encrypted and the password lost. **</u>**



Password

Password ▾

Confirm

Keyfile

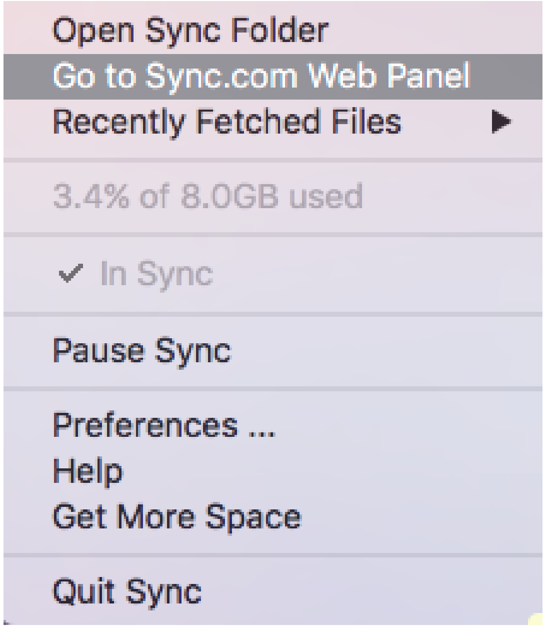
☑ Encrypt also file names (if supported by the format)

☑ Keep password/keyfile for current session

☐ Show password field content

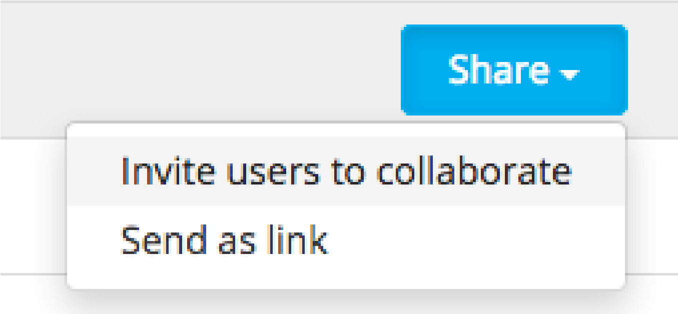
Sharing files with Sync

Open the Sync web panel

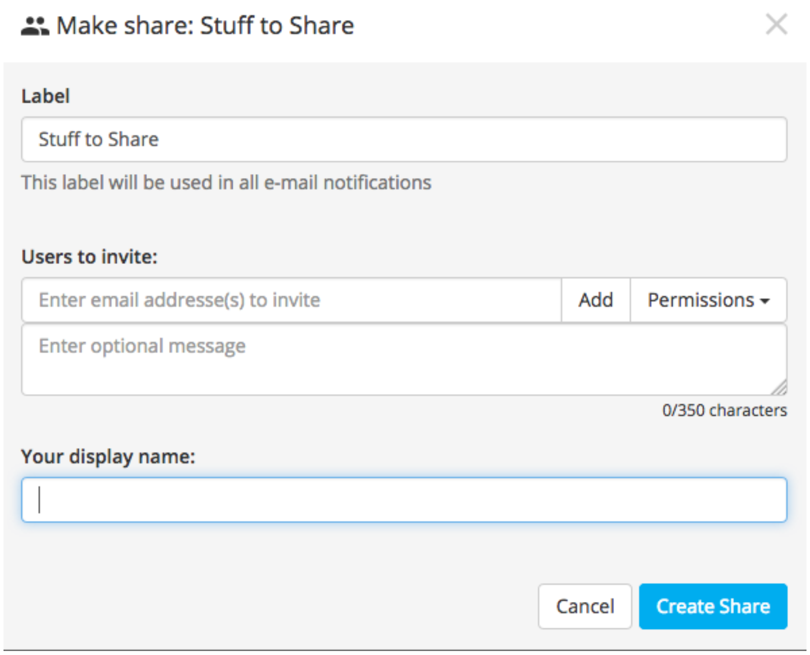


Create a new folder or select the folder you want to share

On the right-hand side of the folder list, select Share



Inviting users



Make share: Stuff to Share

Label

Stuff to Share

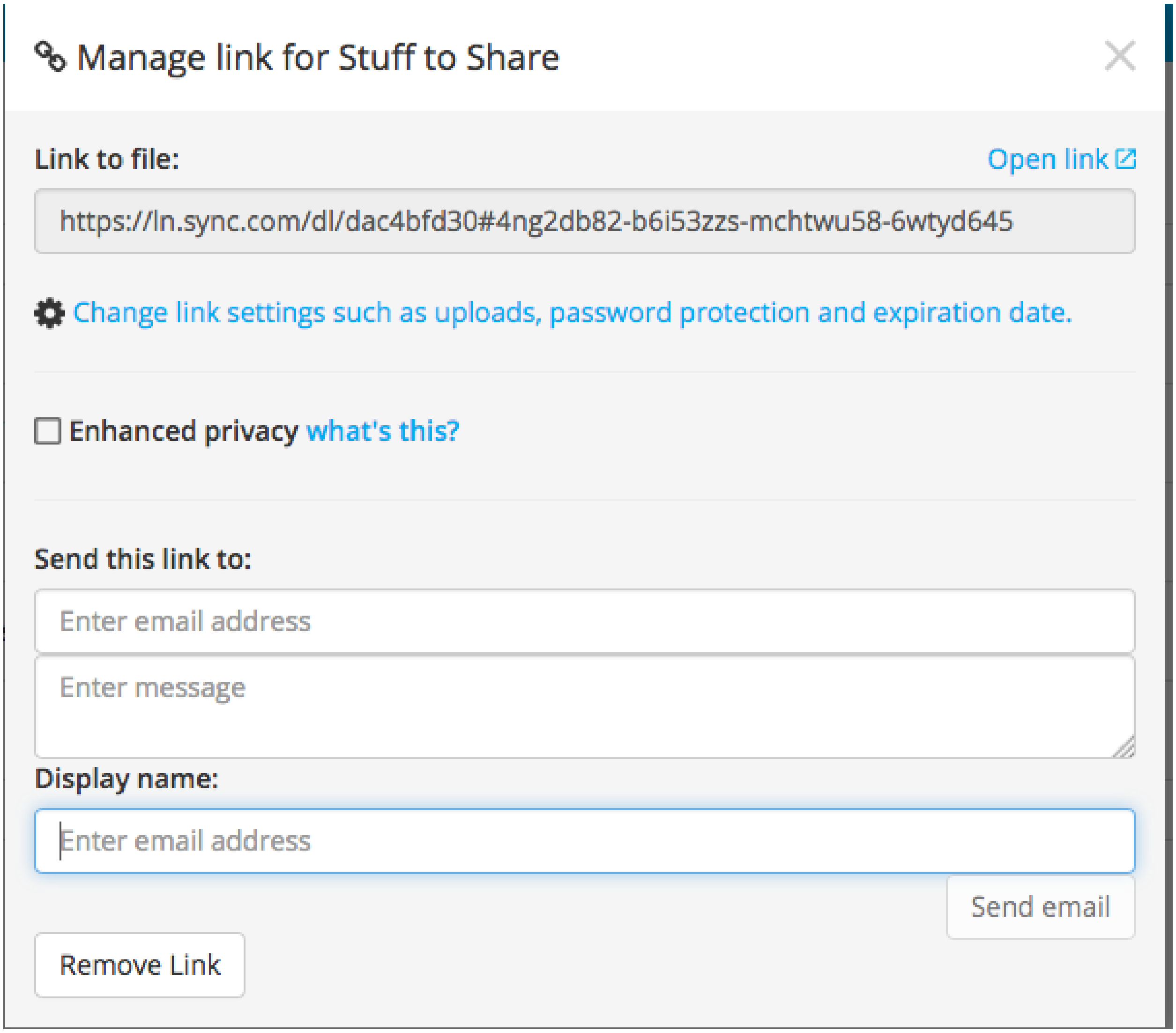
This label will be used in all e-mail notifications

Users to invite:

0/350 characters

Your display name:

Sending a link



Manage link for Stuff to Share

Link to file: Open link

https://ln.sync.com/dl/dac4bfd30#4ng2db82-b6i53zzs-mchtwu58-6wtyd645

Change link settings such as uploads, password protection and expiration date.

□ Enhanced privacy what's this?

Send this link to:

Enter email address

Enter message

Display name:

Enter email address

When users click on the link, they are taken to the folder that you want them to have access to.