UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA
Information Technology Services

Guidelines for the Use of Sync.com Service for Administrative and Operational Activities

Before any personal information can be managed on behalf of the university using Sync.com, please ensure you have read these guidelines and have completed a Privacy Impact Assessment which has approved this use of Sync.com if required. Contact the Information Governance Officer for information about whether your use of the Sync.com service will require a Privacy Impact Assessment.

Any information managed in Sync.com to evaluate a program or activity of a public body must have a Privacy Impact Assessment completed if the information managed is considered Confidential or Restricted as defined below.

If personal information is managed using Sync.com without a Privacy Impact Assessment because of negligence, the individual using Sync.com without approval assumes total personal responsibility for the management of the information using the Sync.com service.

Before starting the use of Sync.com, consider what type of information you are planning to use Sync.com to manage by reviewing the categories below:

Public Information and Data – Minimal Risk and/or Minimal Impact

Description: This is factual information that a reasonable person would feel comfortable posting on a public facing webpage or posting in a public forum. Examples include business contact information and any information that is freely available, such as published marketing materials, public event information and public announcements. This data will not contain any personally identifiable information unless the individual has provided written informed consent that the information can be released to the public.

Using Sync.com to collect, use, store, disclose and dispose of this category of information does not require a Privacy Impact Assessment.

Storage: This type of information can be collected, stored, and disposed of at the user's discretion, with minimal security measures taken. This information can be stored on unencrypted drives and used on public or office devices.

Sharing: This information can be freely shared to respond to routine requests.

Internal - Low Risk and/or Low Impact

Description: Internal data may contain personal information. When personal information is present, the personal information will not be structured to precisely or easily reveal sensitive information about an identifiable person. Personal information if intentionally or unintentionally released would cause a low level of damage to the individual identified. Data may include budgets, advice, recommendations, work schedules, vacation calendars, draft administrative materials and other material that requires approval to be released to the public which does not meet the criteria of Confidential or Restricted.

Using Sync.com to collect, use, store, disclose and dispose of this category of information does not require a Privacy Impact Assessment; however, ***employees are expected to only manage this information in Sync.com with approval from their supervisor.***

Storage: Standard internal information will be stored on devices and drives that are encrypted and password protected. This information and data will be stored on Canadian servers that do not backup information to another country.

Sharing: Standard internal information will be shared only with authorized users. If you are unsure about sharing this information, contact the Information Governance Officer or I.T. Security.

Confidential – Moderate Risk and/or Moderate Impact

Description: This information contains personally identifiable information or aggregated personal health information containing elements that have a low risk of re-identifying individuals. Spreadsheets, databases, or unstructured data revealing standard customer, employee, student or client information with individual identifiers are examples of confidential records.

Using Sync.com to collect, use, store, disclose and dispose of this category of information requires a Privacy Impact Assessment. Contact the Information Governance Officer to begin conducting a Privacy Impact Assessment.

Storage: This information will be stored on devices and drives that are encrypted and password protected. This information will be stored only in locations approved by the Information Governance Officer.

Sharing: This information will be shared only with individuals indicated in an approved Privacy Impact Assessment. Information will be stored in a password protected folder and access only granted to authorized users.

Restricted – High Risk and/or High Impact

Description: Personally identifiable information that can be combined to perform identity theft or create an invasive profile of an individual. Data may include unstructured or structured personal health records identifying an individual. Personal information banks or compiled documents that contain the following information must be classified as restricted information.

- Birth certificate information/photocopies
- Social insurance numbers/photocopies
- Driver's license numbers/photocopies
- Medical service card numbers/photocopies
- BC ID numbers/photocopies
- Passport numbers/photocopies
- Student/work permit information/photocopies
- Temporary resident visa information/photocopies
- Excerpts from/copies of an individual's medical files/history

Using Sync.com to collect, use, store, disclose and dispose of this category of information requires a Privacy Impact Assessment and may require additional approval from the Office of the Information and Privacy Commissioner of British Columbia. Contact the Information Governance Officer to begin conducting a Privacy Impact Assessment.

Storage: This data must be stored on university drives or devices unless approved by the Information Governance Officer. Data and information in this classification must be stored on encrypted and password protected devices and drives and must be stored in a password protected folder or password protected archive file. Contact the IT Security Analyst for instructions to properly securing archive and zip files.

Sharing: This data will not be shared unless authorized by the Information Governance Officer. Passwords for encrypted records will not be transmitted in plain text and will be sent in separate communication from links to the files or folders. The safest method would be to call the recipient and provide the password to the encrypted file over the phone.

Purging documents from Sync.com

Once a record stored on Sync.com no longer requires a legal or operational copy to be stored there, that record needs to be removed from Sync through purging the record. The Sync.com service cannot be used to hold the official copy of any UNBC records except in cases when the Information Governance Officer approves official copies being stored there. Follow the "Instructions on disposing documents from Sync.com" process document to purge documents from Sync.com

Support and Inquiries

Each employee is responsible for the management of UNBC records. The university community does have support to help everyone manage that responsibility. If you are experience technical difficulties with the Sync.com service, use the Sync.com FAQs, Sync.com official user manual and contact Sync.com technical support. If you have any questions about the required data security and information management practices that are not addressed in these guidelines contact:

Data Security Inquiries
Annette Doyle
IT Security Analyst
250-960-6324 (26324)
Annette.doyle@unbc.ca

Privacy and Information Management Inquiries
Adam Cullum
Information Governance Officer
250-960-5139 (25139)
Privacy@unbc.ca