Data Breach & Storage Guidelines

Employees at Mater Christi College access a variety of data and services, located across various vendors and technology.

In accordance with the Australian Privacy Principles (APP), it is required that any breach of private or secure data be reported to the body (Notifiable Data Breach Scheme, 22 February 2018). Mater Christi College is required to ensure data is kept safe to minimise any exposure of private or sensitive data. Acceptance of this policy is in conjunction with the Responsibilities & Acceptable Use Agreement.

The purpose of these guidelines is to make sure all Mater Christi College resources and data are kept within centralised and specified locations and provide reasonable recommendations for how data is accessed and distributed. These guidelines will detail:

- Data Storage Locations
- Additional Storage Technologies
- Email
- Backups
- Responsibilities

The guidelines cover all employees who are responsible for creation, modification and storage of any data used at the College. Students are bound to ensuring their work is kept on the recommended platforms.

Data Storage Locations

The following resources provided should be the only location College/Client data should be kept, unless approved by the Principal.

One Drive

- Individual only, work related drafts, materials, resources and archived file storage.
- Any faculty or department resources should be kept in the provided Team Drives located in Q Drive and S Drive.

Team Drives

- Specific Team Drives have been created for departmental storage of resources.
- This should include department or faculty-based content and curriculum materials.
- Large files that need to be attached to curriculum work in eWorkspace should be linked from One Drive.

eWorkspace

- Files stored on eWorkspace should be classroom materials, current curriculum content, and final submissions.
- Large files must be linked using a shared link from One Drive.

Synergetic

- Synergetic is the College's school management system and as such stores all student, staff and parent private and confidential information.
- Along with the above records, Synergetic allows for safe and secure storage of documents, scanned letters, professional reports and medical files
- Attached files will be kept in DocMan, with certain permissions applied for view edit and upload.

It is strongly recommended that any personal or home data is not to be stored on College services. This includes personal emails, photos or other personal files. Social media accounts should not be linked using your College email account.

Additional Storage Technologies

The above listed technologies are the only College recommended platforms supported. Other mediums for storage will not be supported, and any private or confidential Colleges files must not be located outside of these recommendations.

Other technologies include but are not limited to:

- Network storage
    - this includes Staff Resource folders, shared network drives.
- Local Laptop/hard drive storage
    - all local documents & files must be transferred and kept within One Drive.
    - private and confidential files must not be kept on local storage.
    - downloads and working files must be deleted.
    - exceptions to this rule may include in progress large media files or working files that are required for photo/video work.
        - these files must not contain content which are in breach of the Electronic communication device policy.
        - after a project has been completed, final content must be uploaded to the Team Folder on a Network Drive.
- USB Storage
    - portable USB drives and similar technologies must not contain College documents or materials.
    - Staff & students may only use portable storage for Media classes, ensuring no personally identifiable or private content is kept on these mediums.
- Other Cloud technologies
    - Other providers of online storage are not to be used, as the College cannot provide support; files will be decentralised; service providers may not abide to the Privacy and Security policies as outlined by the APP.

Email

Email services are provided to College using Office 365. Office 365 automatically encrypts and authenticates messages sent from its service. Messages are kept only on the Cloud platform and can only be accessed using the approved website or the Outlook Application for Android and iOS.

Backups

All services and data owned by the College will be routinely backed up to local onsite storage, offsite backup at secondary campus, and online cloud storage providers where applicable.

Responsibilities

The responsibility for ensuring the safety and security of all data resides with all members of the College community. These are outlined below:

Operation Committee – responsible for the evaluation and implementation of the Policy through consultation with members, Future Directions & Leadership.

ICT Department – responsible for the oversight of Technical Services, daily maintenance of the File Servers and the backup procedures ensuring accurate daily/monthly backups.

End users – responsible for the maintenance of their network space to ensure that they are not negatively impacted upon by current allocations. Responsible also for their own external storage devices.

Recommended Password Control

Staff will use passwords to access the College Network as follows:

- Minimum of 8 characters
- Changed every 180 days (6 Months)
- Made up of a mixture of 3 of the following:
    - Alphabetic [A-Z]
    - Capital Letters [A-Z]
    - Non-alphanumeric [!@#$%^&*()]
    - Numbers [1234567890]

Applications

The IT Manager is required to identify and sign off on all applications and where data is stored.

Applications with Identifying Student / Staff Information

Application	Data Location	Privacy URL
Clickview	Australia	https://www.clickview.com.au/privacy-policy/
Synergetic	Australia	https://www.synergetic.net.au/index.php/privacy-policy
eWorkspace	Australia	https://mccportal.materchristi.edu.au/ews/Home/tabid/1/ctl/Privacy/Default.aspx
Google Apps		https://edu.google.com/k-12-solutions/privacy-security/?modal_active=none
Microsoft Office 365		https://privacy.microsoft.com/en-gb/privacystatement
Casper		https://www.jamf.com/privacy-policy/
Papercut		https://www.papercut.com/kb/Main/PrivacyPolicy
Support Centre	Australia	http://www.rtg.com.au/wp-content/uploads/2016/01/RTG-Privacy-Policy.pdf
Adobe	Australia	http://www.adobe.com/au/privacy/policy.html
EdSmart (formerly Parent Paperwork)	Australia	https://www.parentpaperwork.com/privacy
LearningField	Australia	https://www.copyright.com.au/privacy/
CEVN	Australia	https://www.catholicdevelopmentfund.org.au/Privacy?portalid=0
Access-IT	Australia	https://accessitlibrary.com/privacy-policy/
NAB Transact	Australia	https://www.nab.com.au/common/privacy-policy
CompliSpace	Australia	https://www.complispace.com.au/privacy-policy/
Edrolo	Australia	https://media.edrolo.com.au/static/doc/EdroloWebsiteTermsConditionPrivacyStatement.pdf
Rubicon (Atlas)	Australia	https://www.rubicon.com/data-privacy-policy/
SPA Platform		http://www.spaplatform.com.au/terms-privacy

Related Policies

Privacy Policy
Data Breach Requirements
Responsible Uses of Technology Agreement