Guidelines for OneDrive

OneDrive for Business allows users to store files in the cloud, sync those files to devices, and edit and share documents with internal and external users. Although OneDrive for Business is the cloud file sharing solution for the campus, there are security practices that still must be followed to ensure the service is being used properly.

Guidelines for employees using OneDrive for Business:

- OneDrive for Business must not be used for storing any unencrypted campus Level 1 Confidential data.

- This service is not intended for storage of files which might be classified as "confidential" by your academic unit, the University, or for legal compliance. Any “confidential” data must still be limited to IT-managed internal file services.

- Files stored in OneDrive are subject to all University policies including the Campus Appropriate Use Policy, the Storage of Electronic Level 1 Confidential Information Policy, and Section 8000 of the Integrated California State University Administrative Manual (ICSUAM).

- There is no restriction on personal use of OneDrive for Business, but please be aware that there is no guarantee that you will have access to this information if your association with Cal Poly Pomona ends. Also, be mindful of the shared nature of OneDrive before storing any private information.

Best practices for sharing files:

- Use folders to share groups of files with others online.

- Limit file or folder sharing to those with a legitimate educational interest (FERPA) or a valid need to know in order to perform University business.

- Share files with specific individuals, never with “everyone” or the “public”.

- Be careful sending links to files because they can often be forwarded to others who you did not provide access to.

- Remember that once a file is shared with someone and they download it to their device, they can share it with others.

- Remove individuals when they no longer require access to files or folders.

If you have any questions, check with the data owner or your local department policy for additional appropriate use guideline.
## Data Content Confidentiality Levels

### Level 1 – Confidential data
Confidential data includes data which, if accessed by unauthorized entities could cause personal or institutional financial loss or constitute a violation of statute, act or law.

<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| Confidential Information is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Confidential information is information whose unauthorized disclosure, compromise or destruction would result in severe damage to Cal Poly Pomona, its students, or employees. Financial loss, damage to Cal Poly Pomona’s reputation, and possible legal action could occur. Level 1 data is intended solely for use within Cal Poly Pomona and limited to those with a “business need-to-know.” Statutes, regulation, other legal obligations or mandates protect much of this information. Disclosure of Level 1 information to persons outside of the University is governed by specific standards and controls designed to protect the information. | • Passwords or credentials  
• PINs (Personal Identification Numbers)  
• Birth date combined with last four digits of SSN and name  
• Tax ID with name  
• Driver’s license number, state identification card, and other forms of national or international identification in combination with name  
• Social Security number and name  
• Credit card numbers with cardholder name  
• Bank account or debit card information  
• Medical records related to an individual  
• Health insurance information related to an individual  
• Psychological Counseling records related to an individual  

#### Payment Card Industry Data Security Standard (PCIDSS)
- Primary Account Number (PAN) (credit card number) AND any of the following if stored, processed, or transmitted with the PAN:
  - Cardholder Name  
  - Service Code  
  - Expiration Date  
- Vulnerability/security information related to the campus or computer information system  
- Law Enforcement Records related to an individual |
**Level 2 — Internal Use Only**

Internal user data is information generally used internally at the university or with its authorized partners. If released to unauthorized individuals, it would not result in any financial loss or legal compliance issues but would negatively impact the privacy of the individuals named or the integrity or reputation of the University.

<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal use information is information which must be protected due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to Cal Poly Pomona's reputation, violate an individual's privacy rights or legal action could occur. Internal use information is intended for use by Cal Poly Pomona employees, contractors, and vendors covered by a non-disclosure agreement.</td>
<td>• BroncoNumber</td>
</tr>
</tbody>
</table>

**Identity validation keys**
- Birth date (full: mm-dd-yy)
- Birth date (partial: mm-dd only)
- Mother’s maiden name

**Student information**
- Educational records of individual students (Excludes directory information)
  - Home or mailing address
  - Personal telephone numbers
  - Personal email address (not BroncoName@cpp.edu)
  - Ethnicity
  - Gender
  - Birthplace
  - Grades
  - Courses taken
  - Schedule
  - Test Scores
  - Advising records
  - Educational services received
  - Disciplinary actions

Non-directory student information may not be released except with Registrar's Office approval under certain prescribed conditions

**Employee Information**
- Employee net salary
- Employment history
- Home address
- Personal telephone numbers
- Personal email address
- Parents and other family members’ names
- Payment History
<table>
<thead>
<tr>
<th>Employee evaluations</th>
<th>Background investigations</th>
<th>Biometric information</th>
<th>Electronic or digitized signatures</th>
<th>Private key (digital certificate)</th>
<th>Birthplace (City, State, Country)</th>
<th>Ethnicity</th>
<th>Gender</th>
<th>Marital Status</th>
<th>Personal characteristics (e.g., hobbies)</th>
<th>Physical description</th>
<th>Photograph</th>
</tr>
</thead>
</table>

**University Donor Information**
- Name
- Home or mailing address
- Personal telephone numbers
- Personal email address

**Legal Information**
- Legal investigations conducted by the University

**Purchasing Information**
- Sealed bids

**University Research**
- Trade secrets or intellectual property such as research activities

**Library Patron Information**
- Linking a library user with the specific subject about whom the library user has requested information or materials.

**Facilities Information**
- Building plans and architectural drawings

**Other Information**
- Location of assets
Level 3 – Public Information
Data that does not meet the criteria as confidential, sensitive or private as defined above shall be considered non-classified data. Please note that this classification does not imply that the data does not need to be properly managed. Such data may be subject to open records requests.

<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| This is information that is regarded as publicly available. These data values are either explicitly defined as public information (e.g., state employee salary ranges), intended to be readily available to individuals both on- and off- campus (e.g., an employee’s work email addresses), or not specifically classified elsewhere in the protected data classification standard. Knowledge of this information does not expose Cal Poly Pomona to financial loss, or jeopardize the security of Cal Poly Pomona’s assets. Publicly available data may be subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure. | Campus Identification Keys  
- BroncoName (do not list in a public or a large aggregate list, protection of spam)  

Student Information  
- Name  
- Major Field of Study  
- Participation in officially recognized sports/activities  
- Weight and Height of athletic team members  
- Dates of Attendance  
- Full or Part-time status  
- Degrees and awards received  
- Campus E-mail address  
- Most recent or previous college/university/agency attended  

Note: If the student has requested confidentiality via the Registrar’s Office this information is no longer public for that student.  

Employee Information  
- Employee Title  
- Employee public email address  
- Employee work location and telephone number  
- Employing department  
- Employee classification  
- Employee gross salary  
- Name (first, middle, last) (except when associated with protected information)  
- Signature (non-electronic)  

Financial Information  
- Financial budget information