For complete details, please refer to the [Trinity University Information Security Policy](#)

<table>
<thead>
<tr>
<th>CAN BE SHARED?</th>
<th>PUBLIC</th>
<th>PROTECTED</th>
<th>RESTRICTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Yes</td>
<td>• Only with Authorized Users using a secured method (see below)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| EXAMPLES* | • University announcements  
• Press releases  
• Public event details  
• Campus maps  
• Courses of Study Bulletin  
• Academic calendar  
• University public policies |
|-----------|-------------------------------------------------------------|
| EXAMPLES* | • Dates employed  
• Student education history  
• Date and place of birth  
• Student class schedule  
• University ID numbers  
• Library circulation records |
| EXAMPLES* | • Social security numbers  
• Credit, debit, & bank accounts  
• Medical or counseling records  
• Passwords and pin numbers  
• Grade reports & transcripts  
• Individual financial aid records |

| STORAGE REQUIREMENTS | • No limitations or requirements  
• Information is usually available on the University website and social media accounts |
|----------------------|------------------------------------------------------------------|
| STORAGE REQUIREMENTS | • Trinity systems recommended  
• Trinity equipment recommended  
• Cloud storage allowed as long as the files are not made public |
| STORAGE REQUIREMENTS | • Trinity systems ONLY  
• Trinity equipment ONLY  
• Cloud storage ONLY on Trinity-approved platforms (e.g. Drive)  
• Email storage NOT encouraged  
• Security precautions must be taken to protect stored data |

<table>
<thead>
<tr>
<th>TRINITY EQUIPMENT SECURITY</th>
<th>• No restrictions</th>
</tr>
</thead>
</table>
| TRINITY EQUIPMENT SECURITY | • Create strong passwords  
• Lock devices when not in use  
• Never leave a device unattended in a public or unlocked area  
• Log out of devices when done  
• Never share login credentials |
| TRINITY EQUIPMENT SECURITY | • Do NOT store on mobile devices (including TU phones & tablets)  
• Secure your workspace  
• Strong passwords, encryption, antivirus, 2-factor authentication  
• If accessed off-campus, use VDI only on a secured wifi network |

<table>
<thead>
<tr>
<th>PERSONAL EQUIPMENT SECURITY</th>
<th>• No restrictions</th>
</tr>
</thead>
</table>
| PERSONAL EQUIPMENT SECURITY | • Create strong passwords  
• Lock devices when not in use  
• Never leave a device unattended in a public or unlocked area  
• Use antivirus software |
| PERSONAL EQUIPMENT SECURITY | • May NOT be accessed or transferred using a personal device with the exception of VDI  
• If accessed off-campus, you must be connected to a secure wifi network |

| INFO TRANSFER REQUIREMENTS | • Available to share using any method  
• No restrictions on recipients |
|----------------------------|----------------------------------|
| INFO TRANSFER REQUIREMENTS | • May be shared with Authorized Users using Trinity systems  
• If request is external, contact the Data Owner for permission |
| INFO TRANSFER REQUIREMENTS | • Information may be shared with Authorized Users ONLY when required and using only approved, secure methods |

* These are selected examples meant to clarify, not a comprehensive list. Contact Risk Management or the ITS Security Officer if you have questions.