DOS – TIPS TO PRESERVE AND PROTECT YOUR HARD COPY CERTIFICATES:

Use a Protective Folder or Sleeve
Store certificates in acid-free, archival-quality folders or plastic sleeves to prevent yellowing, tears, or moisture damage.

Keep in a Safe, Dry Place
Store documents in a secure location, such as a locked filing cabinet or safe, away from direct sunlight, heat, and humidity.

Request Certified Copies
Obtain certified copies for job or visa applications so you don't have to submit the original unnecessarily.

Digitise Your Certificates
Scan and store high-resolution copies on secure cloud storage (e.g., Google Drive, Dropbox) and on a backup device like a USB drive or external hard drive.

Label and Organise
Label folders clearly (by institution, year, or level) to make retrieval easy when needed for employment, further studies, or immigration purposes.

Authenticate When Necessary
If studying or working abroad, use recognised services such as ACTT's Statement on Recognition to validate the legitimacy of your qualification.

ACTT

DON'TS – COMMON MISTAKES TO AVOID:

Don't Laminate Your Original Certificate

Lamination can damage the document over time and may invalidate it for legal purposes or authentication processes. Embossed (raised) seals can become damaged if pressed under glass or sealed between heated plastic.

Don't Leave in Open or Unprotected Areas

Avoid keeping certificates on desks, under beds, or in folders that are exposed to light, pests, or accidental spills.

Don't Use Staples or Tape

These may tear or permanently damage your certificates.

Don't Share on Social Media

Avoid posting your full certificate online or giving your certificate to unauthorised persons. This could expose personal data and increase the risk of fraud or identity theft.

Don't Submit Originals Unnecessarily

Always ask if a certified copy would suffice. Only submit an original certificate to a reputable organisation if explicitly required; do request that it be returned in a timely manner and in proper condition.

ACTT

SAFEGUARDING YOUR DIGITAL AND ELECTRONIC CERTIFICATES

Store in a Secure Cloud Drive
Use encrypted cloud services like Google Drive, OneDrive, or Dropbox with two-factor authentication.

Use a Smart Card to store your Private Keys and Digital Certificate
The keys are created and stored on the card, so they're never saved on your computer or hard drive – keeping them safe from hackers. Only someone with your PIN could use the card, so keep the smart card and PIN secure to prevent misuse.

Record Metadata Separately
Keep a separate record (in a secure note) of details like the issuing authority, date earned, certificate ID, and verification URL.

Backup to Encrypted USB Drive
Save a copy on a password-protected and encrypted USB drive as an offline backup.

Enable Device Encryption
Ensure your computer or phone uses full-disk encryption to add a layer of protection.

Avoid Sharing Publicly
Never post your full certificate or credential ID on social media or public websites.

Keep Software Up to Date
Use updated antivirus and system software to protect against theft or corruption.

Digitally Sign or Watermark Personal Copies
If sharing a copy (e.g. for job applications), add a subtle watermark or digital signature to prevent misuse.

Use Read-Only or PDF Format
Store your certificate as a non-editable PDF to maintain its integrity and prevent unauthorised modification.

ACTT