COLLOQUIZE

Deleted data retrieval checklist

What to do when data has been deleted or lost: protect the chance of getting it back.

- [ ] 01 **Stop using the affected system**
  Every write can overwrite deleted data. Shut down a single laptop or drive rather than carrying on.

- [ ] 02 **Do not repair or reformat**
  No disk repair, reinstall or factory reset. Never install recovery software on the affected drive.

- [ ] 03 **Write down what happened**
  What was deleted, when, by whom or what, where, and what has happened since.

- [ ] 04 **Preserve the original**
  Make a bit-for-bit image, ideally through a write blocker, and work only on the copy.

- [ ] 05 **Check the easy sources first**
  Recycle bin, version history, backups, snapshots, cloud recoverable items, database point-in-time recovery.

- [ ] 06 **Know what your storage means**
  HDDs may keep data until overwritten; SSD TRIM, encryption (you need the keys) and cloud retention change the odds.

- [ ] 07 **Leave physical failure to specialists**
  Clicking, undetected, dropped or water-damaged drives: power off. No home fixes.

- [ ] 08 **Treat deliberate deletion as an incident**
  Chain of custody, hash the images, involve security, HR or legal. Personal data loss may be a reportable breach.

- [ ] 09 **Handle recovered data as sensitive**
  Encrypt, limit access, restore to a clean place, verify. Do not restore data deleted on purpose (erasure, retention).

- [ ] 10 **Close the gap afterwards**
  Tested restores, versioning or soft delete, limited delete rights, change control, mass-deletion alerts.

If in doubt, stop

Leave the affected device or system alone, write down what happened, and ask for help before trying fixes. Nobody can promise recovery, but you can avoid making it harder.

Full guide: colloquize.com/insights/data-retrieval-best-practice.html Contact: info@colloquize.com
General guidance, not legal advice. Colloquize, 20 October 2026.