



## Data Shredding Policy

This data shredding policy outlines how St Paul's church will destroy data when it is no longer needed. The policy includes what type of data will be destroyed, how it will be destroyed, and who will be responsible for destroying the data. Having a data destruction policy ensures that retired devices and media have their contents securely removed, destroyed, or overwritten so that it is extremely difficult or impossible to later retrieve data.

This data destruction policy affects:

- Paper copies
- Mobile Phones: iPhones, Androids, Blackberries, etc
- Hard drives, flash memory devices,
- CDs, DVDs, Blu-Rays, and other tape storage drives

As with paper records, most electronic records should be destroyed after an appropriate time period, rather than being stored indefinitely. This period is set out in the Data Retention Policy.

1. Any printed data that is to be disposed must be safely disposed of by crosscut shredding. Any group which does not have access to a crosscut shredder should pass material to the Church Administrator who will undertake secure shredding.
2. Mobile phones usually do not have a standardized way to securely delete or remove their data. However, most phones will have a "hard reset" or "cold reset" button which will remove software and restore the handheld device to factory default settings. After resetting the device, check to ensure that no church data remains on the phone before discarding.
3. Special care must be given to disposing of data stored in electronic media. Guidance will be given by the Church Leadership team to any group which has stored personal data relating to its members on, for example, personal computers which are to be disposed of:
  - a. Destruction of electronic records: Simply deleting a file will not necessarily prevent it from being recovered by an expert user. Before disposing of any computer hardware it is therefore important to completely clear the hard drive, and if throwing away (for added security) physically destroying it. Alternatively, the local Recycling Centre has a data shredding secure box for PC hard drives etc. Do not dispose of a computer without removing the hard drive or using a reputable data shredding app to wipe the hard drive clean eg Darik's Boot and Nuke (DBAN) or Disk Wipe. If you require any assistance, please contact the church administrator.
  - b. Archiving of electronic records: You must remember that as part of any backup procedures you have in place there must be provisions for the deletion (or overwriting) of your backups. Consider how long it is necessary to maintain your backups for and then put in place a continual cycle to regularly delete or overwrite the data.
4. CDs, DVDs, Blu-Rays, and other tape storage drives. All optical and tape media should be physically destroyed when they are no longer necessary.