RCCG Palace of Grace Parish, Eastleigh
Data Retention Policy and Data Disposal Procedures

1. **Scope**

RCCG Palace of Grace Parish, Eastleigh requires that all removable storage media are clean (which means it is not possible to read or reconstitute the information that was stored on the device or document) prior to disposal.

2. **Responsibilities**

1. The Support Services Manager is responsible for managing the secure disposal of all storage media in line with this procedure when they are no longer required and is responsible for the management of any company engaged by **RCCG Palace of Grace Parish, Eastleigh** as the approved contractor for removing shredded documents.
2. All *owners* of removable storage media are responsible for ensuring that these media are disposed of in line with this procedure.

3. Retention Policy

3.1. **RCCG Palace of Grace Parish, Eastleigh** will retain the information provided and only share with those it is legally entitled to. The information will only be kept for as long as necessary.

3.2. The retention period of records we hold differ and are subject matter specific. **For instance, the table below gives some examples:**

Document	Reason for retention period	How long to keep (minimum)
Application forms and interview notes (unsuccessful candidates)	Disability Discrimination Act 1995 and Race Relations Act 1976 recommend six months. One year limitation for defamation actions under Limitations Act	Six months to a year
Payments cash book or record of payments made	Companies Act/Charities Act	Six years from the end of the financial year in which the transaction was made.
Invoice – capital item	Companies Act/Charities Act and HMRC	Ten years

4. **Procedure for Disposal**

4.1. Hard disks must be cleared of all software and all organisational information prior to disposal or reuse, as set out in Clause 3.5 and 3.6, below.
4.2. The Support Services Manager is responsible for the secure disposal of storage media and the disposal of all information processing equipment is routed through their office. A log is retained in the Support Services department showing what media were destroyed and/or disposed of, and when. The information asset inventory is adjusted once the asset has been disposed of.
4.3. Hard disks are cleaned using [insert details of technology and process] and [insert details of any process used to verify that they have been cleaned].
4.4. Hard disks are cleaned by [insert details of external service provider] who guarantee [insert details of level of cleaning and process used for verification].
4.5. Devices containing confidential information [dependent on a risk assessment] are destroyed [how?] prior to disposal and are never reused.
4.6. Devices containing [confidential] information that are damaged are subject to a risk assessment prior to sending for repair, to establish whether they should be repaired or replaced.
4.7. Portable or removable storage media of any description are destroyed [how?] prior to disposal.
4.8. All media are disposed of in line with [local jurisdictional] regulations [which are what?] on disposal of computer equipment, through (Insert Parish Name) approved contractor [who?].
4.9. Documents containing *[confidential]* and *[restricted]* information that are to be destroyed are shredded by their *owners*, using a shredder with an appropriate security classification. These shredders are located *in the open plan office*. The waste is removed by the approved contractor.

Document Control

The Information Security Manager is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the GDPR.

A current version of this document made available members of staff by email and is published in the RCCG Palace of Grace Parish, Eastleigh internal Compendium of Policies.