

**Data Protection Policy**

Created: July 2016

Updated: July 2018

**Purpose**

The purpose of this policy is to make staff aware of the main requirements of the Data Protection Act 1998 and also the General Data Protection Regulation and Data Protection Act 2018.

The Data Protection Act places responsibilities on all staff who have access to information held on computers or other automatic systems. This is virtually all of us.

The Act includes eight principles which must be followed by all data users. Briefly, these principles state that personal data should:

• be collected and processed lawfully and fairly. No-one should be misled about the purposes of personal data which is obtained from them or the extent to which it may be disclosed.

• only be used for registered purposes.

• be adequate and relevant for its registered purpose

• be accurate and, where necessary, kept up-to-date.

• Not be kept for longer than is necessary for the registered purposes. Obsolete data can be kept separately from current files for specified purposes, but data which is no longer needed should be deleted.

• be open for data subjects with access at reasonable intervals to data which relates to them and, where appropriate, to have it corrected or deleted.

• Be secure against unauthorised access, alteration, disclosure or destruction and guarded against accidental loss or damage.

The school has registered in the name of Christ Church with the Data Protection Registrar its uses of all ICT systems which hold personal details.

The utmost care must be taken with personal data and the school trains all staff in General Data Protection Regulations (GDPR). Generally speaking, it may be disclosed to any other member of staff at Christ Church who needs it for one or more registered purposes but there is a clear understanding of keeping these details private. It should not be disclosed to external persons or organisations unless these types of disclosures have been registered and the disclosure agreed by the Senior Management Team.

Personal data must not be obtained from unauthorised sources nor used for unauthorised purposes. Great care should be taken about data received over the telephone and even greater care over providing information in this way. The general advice must be – Do not give information over the phone – ask the caller to write.

Disclosure of information is not limited to any particular method. V.D.U. displays, printed or handwritten data, microfiling and spoken disclosures are all relevant, provided the data is held on a computer file in the first place.

Personal data is not limited to what may be thought of as “highly confidential”. For example, names, addresses and telephone numbers, marital status, occupation are all types of personal data.

For further information on data protection, the school refers to ‘Data protection: a toolkit for schools 2018’. This document gives specific guidance, including 9 essential steps, to help effectively manage data protection.

**Subject Access Provision**

Where there are already existing arrangements for people to see records, apply these arrangements strictly and do not give additional information if someone claims entitlement to this under the Data Protection Act. If this is the case the subject access request procedures must be carried out.