BISHOPS' CONFERENCE OF SCOTLAND

BASIC GUIDE TO DATA PROTECTION

Table of Contents

Document Control

Title	Basic Guide to Data Protection
Prepared by	Donna Maguire
Approved By	Monsignor Hugh Canon Bradley
Date of Approval	22 March 2018
Version Number	1.2
Review Frequency	Every 3 years
Next Review Date	March 2021

Status Control

Version	*Date*	*Status*	*Prepared by*	*Reason for Amendment*
1.2	11/2/2018	Complete	DMM	

BASIC GUIDE TO DATA PROTECTION

This guide is intended to help you understand and put into practice the Bishops' Conference of Scotland's (BCOS) Data Protection policy in your day to day work. Please make sure that you have read and understand the Data Protection Policy.

The **General Data Protection Regulation** (GDPR) exists to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge and, wherever possible, is processed with their consent.

Personal data is information about a living individual by which that individual can be identified. This includes factual information that expresses an opinion about them. It can be in any format, including images and audio-visual material.

Information processing includes just about anything an organisation does with the data, even just holding it on its computer system or filing system.

1 KEEPING PERSONAL INFORMATION SECURE

If you hold personal information about living people, you must make sure that it is safe, secure and cannot be accessed by unauthorised persons. You should:

- change your computer password regularly and do not share it with others
- lock or log off from your computer when you are away from your desk
- make sure that hard copy personal information is securely stored when not in use: do not leave it on your desk
- be aware of who might be looking over your shoulder; check who can see your screen; have you left any documents on your desk?
- make sure that visitors are signed in and out of the building and accompany them in office areas
- ensure that all personal information about third parties is saved in an appropriate place.; personal information about yourself should be in your personal folder on the hard drive; do not save any personal information to your computer hard drive
- think carefully about taking any personal information outside the building if its loss could cause damage or distress; if this is absolutely necessary, ensure that electronic information is encrypted, or password protected
- when working outside the building or using a personal computer, tablet or phone, ensure that you are working within the remote desktop as far as possible
- if you access work emails or documents using a mobile phone, ensure that it is password protected and you have installed an application which enables remote wiping. (Further information on this is available from the BCOS IT provider).

- if you have reason to believe that any personal information has been lost or stolen, inform your line manager, the BCOS General Secretariat or the Archivists at once. (If this is because you have lost your computer or phone, you must also inform the BCOS IT provider.)

2 MEETING EXPECTATIONS ON DATA PROTECTION

Your colleagues and external contacts have a right to expect that their personal information is managed by the BCOS in a responsible and compliant way. You should:

- only collect personal information that is necessary for a specific purpose (e.g., you will need someone's address and bank details to process an expense claim, but not their age or marital status)
- make sure that people are aware of what their personal information will be used for and that you have sought their consent in an appropriate way. (Further guidance on how to seek consent is available in the document 'Data Collection Form templates'.)
- inform people and seek consent if this use changes
- delete personal information that is no longer required
- update records promptly if requested by the individual concerned.

3 DISCLOSING INFORMATION

Be aware that unscrupulous individuals or organisations may try and trick you into giving out your own, or someone else's, personal information. You should:

- never share someone else's personal information unless you have obtained their prior consent
- never give out personal information over the phone unless you are absolutely certain of the identity of the person to whom you are speaking
- as far as possible, deal with matters concerning personal information in writing
- ask a person to provide proof of identity if you are unsure about who you are dealing with
- speak to your line manager or archivists if you are at all concerned about a request for information before releasing information. When on the phone, offer to ring the person back or ask them to email or write in.

4 SUBJECT ACCESS REQUESTS

A person has a right to a copy of any of their personal information that you hold. The GDPR allows them to ask for this by making a **Subject Access Request**. This must be replied to within 30 days, including weekends and bank holidays. There is no longer any financial charge for a subject access request.

In theory, any request in writing by an individual for information you hold about them could be a subject access request. In practice, if what they've asked for is something that you would normally deal with as part of day to day business, deal with it in your usual way

e.g., What *address do you have on file for me? How much do I owe for these publications? What date did I finish working here?*

However, if you have a request that is unusual compared to what you deal with day to day, particularly if it asks for a large amount of information, information covering a long period of time, mentions a 'right to' or 'obligation to provide' information, the information requested includes a third party's details, or you are uncertain about the person's identity, then it may be appropriate to deal with it as a subject access request. e.g. *Please provide a copy of my staff records. I have a right to see these. Please could I have all the invoices you have issued to me in the past five years. I am acting on behalf of my client and need a copy of all his correspondence with your organisation. A written authority is enclosed.*

If you think you have received a subject access request, bring it to the attention of BCOS HR or the Archivists. If we think it really is a subject access request, then it will be answered centrally, though you will be asked to provide the relevant information. In some cases, we may ask you or someone in your department to answer it but, if this happens, you will be given advice and instructions.

5 FURTHER ADVICE

The ICO (Information Commissioner's Office) has provided this guide on Data Protection for organisations: https://ico.org.uk/for-organisations/guide-to-data-protection/, as well as this guide to GDPR for organisations: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The Bishops' Conference of Scotland provides further related advice, in these following areas:

Guide to Data Protection and the Use of Photographs
Data Protection Policy
Data Collection Form Templates
Privacy Statement
Confidential Waste Disposal Policy
Retention Schedules
Email Policy
Use of Personal IT equipment
Working offsite
Information Audit Form and Guide
Data Subject Request Form