Bristol Cathedral

DATA PROTECTION CODE OF CONDUCT – VOLUNTEERS

May 2018

Introduction

This document sets out the code of conduct which is expected of anyone volunteering in the Cathedral in relation to data protection. It should be read in conjunction with the Cathedral's Data protection policy and privacy notice. The code enables us to ensure that the Cathedral is compliant with the General Data Protection Regulation and other legislation. This code applies to volunteers.

Keeping personal data safe

All those volunteering in the Cathedral have a responsibility to keep people's personal data safe. We have set out below what people should and should not do to fulfil their responsibilities.

what you need to do	how to do it	notes
keep electronic and hard copy records safe at home	electronic data – on a home PC - change your password quarterly on your PC - lock your PC or laptop (control/alt/delete and select lock) when you are not at your desk - only use your cathedral e-mail account for cathedral related work - use password protected files/spreadsheets where the data is sensitive (e.g. financial) - shut down your computer when you are not using it hard copy - please keep files with personal data related to the cathedral in lockable cabinets if possible - use shredders if you have them for waste disposal **DO NOT** - share your passwords with anyone - leave written passwords around the desk/PC Be careful about who has physical access in your home to your information/files.	we will be providing a cathedral e-mail address for our volunteer leaders so that you can access our secure systems via the web if you have a large quantity of hard copy data from your cathedral work and you wish to dispose of it safely then use the cathedral confidential shredding bags – Gatehouse – see Chrissie Graham

keep electronic and hard copy records safe when out for meetings/over night visits	electronic data - make sure any laptop/digital device is locked when not in use - do not use unsecure wi-fi hotspots unless strictly necessary – use the 4G network for internet access if you can - be aware of people around you who might look at your screen –'shoulder surfing' - and people who may take photos of your laptop/other equipment hard copy - keep meetings papers in folders and do not leave papers unattended on the train/other transport - only take the paperwork necessary for the meeting/immediate work and avoid taking sensitive data unless strictly necessary (e.g. safeguarding meeting)	either turn the wi-fi off on your mobile phone when you are out and about, or set it so that your phone notifies you about networks, rather than connecting you automatically – this should be done in settings under the wi-fi buttons
respect confidentiality	- do not make sensitive telephone calls in the company of others – use an empty office or meeting room if necessary - do not have sensitive conversations in front of other people or on public transport/places – particularly if pastoral/personal	
protect people from data breaches	**REPORT a data breach** or concern if something goes wrong and we will assess what action needs to be taken – if you accidentally send an email to the wrong person either recall it or ask the person to delete it – if you think there is any risk to an individual in terms of who the email has gone to then complete report it to Andy Webb More serious breaches to potentially need to be reported to the individuals who could be affected. Examples would include: – you lose a lap top/USB stick or its stolen which has cathedral data on it – if it was locked it will probably be OK, but if not then we would need to take some follow up action – you leave your papers on a train – we would need to alert people and try to retrieve them if possible – you're home PC is hacked and there was cathedral information on it – we would discuss the severity and take advice	if you need to **recall an e-mail message** click on the message itself make sure you are on the message tab half way along the top bar you will see 'Actions' with a drop down menu select the menu and choose recall this message the recall may be successful, but sometimes people will have already seen the message – do the best you can and ask others to delete the message this is for a Microsoft/outlook system – but other email systems should have the same capacity

	– there's a major external hack through our systems – we would need to alert individuals and also the ICO/Charity Commission	
	E-mails - if in doubt **NEVER** click on attachments or answer requests for personal data/financial information etc. - go to a web browser and put in the site you wish to visit directly if you wish to check the authenticity of a site and to avoid mirror/false sites that look the same as the real thing	be careful about the tone and wording in your e-mails as individuals can now request to see their data under Subject Access Requests – volunteers should use a business like tone in e-mails and documents
	Personal electronic devices if you have your email on your personal tablet or mobile phone please - use a PIN/other security measure to secure the device - make sure you keep up to date with software upgrades from your provider - if your phone is lost/stolen and it contains cathedral data please let us know	contact details andy.webb@bristolcathedral.co.uk 0117 946 8187
	Home PC - if you have any cathedral data on your home PC minimise the amount of data held and delete what is no longer required - make sure you keep your anti-virus software up to date and keep up to date with software upgrades - if you have a serious hack/problem with your home system and you have cathedral data on the system please contact Andy Webb	
share information appropriately	- you will need to use your cathedral contacts to manage volunteer activity – e.g. rotas and arrangements - volunteers have given us consent for the use of their data for these purposes and new volunteers will be asked to complete the forms when they join us - therefore – you can e-mail/phone each other when you are doing cathedral work, but you should not give any personal contact details to other people/third parties without the consent of the individual	we will be providing more detailed guidance on this soon

	- DO NOT give out/send the staff contacts list to anyone – never give out the home phone numbers – these are for internal/emergency use only - do not share people's personal mobile phone numbers without consent – you can contact the relevant person and ask them to get in touch with someone who is happy for you to share details - **NEVER** share any contact details/information for volunteers who are under 18 – always copy parents in on communications	
assess the impact of new work on data protection	data protection impact assessments will be completed when the Cathedral plans or begins a new activity or project which will involve personal data or have an impact on personal data we will complete any necessary assessments and discuss them with volunteer leaders/coordinators as required	see policy for examples
make sure everyone has training	the national church has developed a training programme which we will roll out to volunteers	
report concerns	as with other compliance issues volunteers should report any concerns about data protection compliance to Andy Webb in the first instance, and the Chapter Clerk if necessary for action	