Bristol Cathedral

DATA PROTECTION

DATA POLICY AND PRIVACY NOTICE

May 2018

1. This is the data policy and privacy notice for the Cathedral of the Holy and Undivided Trinity, Bristol. It was approved by the Dean and Chapter on 16 May 2018.

Legal context

2. Our policy enables the Cathedral to be compliant with the following legislation:

- The Data Protection Act (1984, 1998)
- 2003 Personal and Electronic Communications Regulations (PECR)
- 2016 General Data Protection Regulation (GDPR 2016/679)
- National church guidance on the retention of Cathedral records ('Chapter and Verse 2013')
- The Cathedrals Measure (1999) and Care of Cathedrals Measure (2011)

3. Data protection legislation exists to protect individual privacy, keep people's personal data safe, and to protect them from potential harm (e.g. fraud). Article 5 of the GDPR requires that personal data shall be:

- processed[1] lawfully, fairly and in a transparent manner
- be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary
- accurate and where necessary, kept up to date
- kept for no longer than necessary
- be protected by appropriate security measures to prevent loss or unauthorised access

4. We have to have a lawful basis for processing personal data. These are:

- consent (individuals have given explicit content for data processing and sharing)
- contract
- legal obligation (e.g. HR and compliance)
- vital interests (e.g. where someone's health is at risk)

[1] Processing includes – obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, matching, transmitting, disseminating, making available, aligning, combining, blocking, erasing, destroying. ICO guidance 2017.

- public task (e.g. public functions like marriage services and funerals)
- legitimate interests (e.g. the management of membership schemes)

5. An individual has the right to:

- access records
- request the erasure of records
- request the rectification of records
- request a restriction of processing activity
- object to processing
- have automated data provided for other uses
- complain

6. Key definitions are set out at Annex A.

Our commitment to data protection

7. The Dean and Chapter takes its responsibilities as a data controller and processor seriously. We are committed to ensuring:

- That we have the necessary policies and processes in place to manage data protection well.
- That we have the necessary infrastructure (ICT etc.) in place to keep people's data safe.
- That we will train our staff and volunteers in good practice.
- That we will ensure that only the appropriate staff and volunteers have access to personal data and that people or contractors do not use any personal data for their own purposes. We will have written agreements in place with our third party contractors to govern the data relationship.
- That we will be responsive to those who raise concerns about data protection or who make requests.
- That we will minimise the amount of information we collect and keep.

8. The Cathedral has never, and will not, sell any personal data to third parties or advertisers and nor do we use any external agencies for fundraising. We do not collect Cookies on our website.

Roles and responsibilities

9. The responsibilities are as follows:

- Bristol Cathedral is a registered data controller with the Information Commissioner's Office.
- The Dean and Chapter have the responsibility for ensuring that data policies and procedures are in place and that compliance is managed proactively. Chapter will review the policy on an annual basis and will receive an update on compliance issues at each meeting.
- The Chapter Clerk has the management responsibility for ensuring the system and procedures are in place.
- The Finance Manager acts as the Data Protection Lead and is responsible for the management of the Cathedral's database.

- The Cathedral maintains a database and provides data processing services to Bristol Cathedral Trust and the Friends of Bristol Cathedral which are both independent charities. A memorandum of understanding with each covers the service provided and the responsibilities of each party.
- The Cathedral also has a CCTV system – a separate policy governs its use, which can be requested from dataprotection@bristol-cathedral.co.uk.
- This policy covers the Cathedral staff, volunteers and all individuals who come into contact with the Cathedral.

Contact details for the Data Protection Lead are: dataprotection@bristol-cathedral.co.uk, 0117 946 8187.

Personal data

10. The Cathedral holds personal data for staff, volunteers, members of the church community, contractors and suppliers and individuals (members of the public or visitors). **The electronic and hard copy data we hold may include:**

- contact information – where you live or work and how to contact you
- consents – preferences for marketing and fundraising
- financial – for giving and other purposes
- national identifier – National Insurance number
- sensitive data[2] – including socio-demographic and criminal records (safeguarding and HR)
- medical – allergy/medications/emergency contacts
- security – CCTV footage
- communications – what we learn from e-mail and other correspondence

11. We use personal data for the following functions:

- to manage the governance and organisation of the cathedral's day to day work
- to organise and manage the delivery of services of worship
- to organise and manage the delivery of events and activities
- to organise and manage our pastoral support programme
- to organise and manage our commercial activities (shop and café)
- to manage our legal responsibilities in relation to safeguarding, health and safety, data protection and human resources
- to manage our membership schemes (Fitzhardinge Society and the Friends of Bristol Cathedral)
- to promote our events and activities (marketing)
- to manage our financial processes for staff, volunteers and suppliers
- to fundraise for resources to support our work
- to organise and manage projects in the cathedral (e.g. fabric related)
- to evaluate our work and efforts and inform wider research

[2] factors including; physical, psychological, genetic, mental, economic, cultural or social, sexual, political, philosophical and religious, details of criminal convictions or allegations

12. Where necessary, and it is appropriate, we may share some data with third parties for the purpose of managing our day to day work. These third parties will usually include:

- cathedral volunteers – who are managing events and activity
- partner organisations – who are managing events and activity (e.g. a local charity)
- statutory bodies – to meet legal requirements (e.g. HR/safeguarding) – e.g. Police, social services
- service providers – e.g. suppliers and contractors who support the delivery of worship, events and projects

13. We work to keep personal data safe by:

- Having robust arrangements in place to protect our electronic and communications systems from hacking and other suspicious or dangerous activity. This includes specialist software and a helpline for staff. All our systems are held on UK/EU based data servers and our ICT systems are maintained by reputable ICT companies.
- Having a single database which keeps all our core communications data in one place. A password is required for use and only authorised staff are given access to the database. The system has been designed to minimise the access to personal data. Super users can access a range of data, but lower level users can only access basic information (e.g. contact details). Subscription mailings (e.g. marketing and fundraising) are only sent via our official system (e.g. mail chimp). We do not hold full bank details on our card payment machine (café).
- Having a code of conduct for staff and volunteers which sets out good practice in terms of data protection, including the use of passwords for the ICT system and lap tops and protected USB devices for electronic information, and security measures for hard copy information,.
- Training our staff and volunteers in good practice.
- Staff and volunteers can flag any issues or concerns with the Data Protection Lead or their managers and if there was a serious issue we have a whistle blowing policy (staff handbook).
- We have a data protection risk assessment which will be reviewed by the Health and Safety Committee on an annual basis.

Procedures

Right to request – managing and changing your data and preferences

14. Individuals should e-mail **dataprotection@bristol-cathedral.co.uk** if you wish to:

- **have your contact information and preferences deleted from our database**
- **update your preferences for communication (e.g. marketing information)**
- **ask us to make some changes to the information we hold on you (including rectification or erasure)**
- **ask us to restrict the way we process your data, or withdraw your consent to processing**

15. Each request will be considered on a case-by-case basis. In some instances we may not be able to delete all records as other issues and legal requirements may be a factor. For example some records need to be kept for safeguarding, HR, financial and other purposes. If necessary we will take expert advice from

the Information Commissioner's Office to ensure correct processing. We will also action any requests from the **Fundraising Preference Service** to change individual preferences or delete data as required.

For rectification, erasure or restriction requests we are required to respond within one month, but this can be extended to two months if it is a complicated situation. We also have to notify the people who have received the information of the change to individual preferences. In most cases this would mean us asking staff, volunteers and contractors to delete information they might hold and to change future communications. We are allowed to make a decision about what constitutes a reasonable effort in these circumstances. The Data Protection Lead is responsible for making sure we have complied with any requests.

16. Once we have deleted information from our e-mail server it can take up to 90 days for the records to be finally deleted, as the servers hold them temporarily and then automatically delete them at the end of that period.

17. The Cathedral does not have any automated decision making and profiling processes.

Data breaches

18. A personal data breach "means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data"[3] This includes breaches that are the result of both accidental and deliberate causes. The process for reporting a data breach depends on the severity and the risk of harm and cases are considered on an individual basis. Low level mistakes that are unlikely to cause any harm do not necessarily need to be reported to an individual. However, more severe and/or risky situations do require notification. Examples of more serious breaches in the Cathedral context could include:

- Our ICT firm detects an attack on their, or our network, and informs us that Cathedral data has been unlawfully accessed.
- A loss of personal data because a member of staff loses a work lap top or passcode protected USB device.
- The loss of hard copy/paper files due to accident (e.g. flood), theft, or other means.
- A volunteer's home computer being hacked which contains Cathedral data.

19. Cathedral staff and volunteers will be asked to keep a personal record of low level incidents, such as a mis-sent e-mail, and to record more serious breaches on a form which is then submitted to the Data Protection Lead for action. Serious cases will be escalated to the Chapter Clerk and in the most serious circumstances the Charity Commission and Information Commissioner's Office would be informed. The specific action taken will depend on the specific circumstances and advice from our ICT suppliers.

[3] Definition from the ICO 'Guide to the General Data Protection Regulation'

Subject Access Requests

20. Under the data protection legislation individuals can make a 'Subject access request' to an organisation.

What can I request?

21. The request allows individuals to get a copy of the information held about them by the Cathedral. The individual is also entitled to be:

- told whether any personal data is being processed
- given a description of that personal data, the reasons it is being processed and whether it will be given to any other organisations or people
- given a copy of the personal data
- given details of the source of the data (where this is available)

How do I make a request?

22. The request needs to be made in writing – it is up to the individual whether this is done by correspondence or e-mail. You have the right to request the format in which you want the information to be provided.

23. Correspondence should be sent to the Data Protection Lead, by hard copy to Bristol Cathedral, College Green, Bristol, BS1 5TJ, or by e-mail to dataprotection@bristol-cathedral.co.uk.

How does the Cathedral respond?

24. The Data Protection Lead or another member of staff will acknowledge the request within five working days or less. We have one month to provide the information request, but this can be extended to two months in complex cases. We will respond to the request with an outline of when the information can be provided. The Cathedral is allowed to make a charge for the request in certain circumstances, which must be based on the administrative cost of the work. We would provide an estimate of the cost for an individual to consider.

Data protection impact assessments

25. Under the GDPR legislation organisations should complete data protection impact assessments when considering new projects, to make sure there are no adverse effects on people's privacy or rights from the new project or work taken forward. In the Cathedral context we would generally complete an impact assessment for the following reasons:

- When considering any changes to the way our ICT and communications systems are managed and run – this includes e-mail and web based systems.
- When considering new software and hardware purchases that would involve migrating data to new systems. This would include any major changes to the Cathedral database and our inventory systems.
- When we might do new marketing or communications activities.
- When we develop and launch any fundraising campaigns.
- When we want to participate in any research activity, commissioned by the Cathedral or third parties.
- When the change would have an impact on sensitive data – e.g. staff information or other records.

Making a complaint

26. If you wish to make a complaint about our data protection policy or processes please e-mail dataprotection@bristol-cathedral.co.uk or ring 0117 946 8187.

27. We take complaints seriously, and will aim to resolve the issue in a constructive and positive manner.

28. We will acknowledge receipt of the complaint within five working days or less. We will provide an answer to the issue as quickly as possible. If the complaint requires us to take additional advice, for example from the Information Commissioner's Office, we will advise you of the timeline for resolution.

29. If you do not receive a satisfactory reply from our Data Protection Lead you can ask for the request to be escalated to the Chapter Clerk and Dean (0117 926 4879). In the most serious situations Chapter (the Board) would be responsible for making a collective decision on the Cathedral's response. The Chapter Clerk would take the lead for communicating with the complainant in more serious matters, setting out the timetable for the Cathedral's response and proposals for a resolution.

30. If there was further concern then complainants should put the issue in writing to the Bishop of Bristol, who acts as the Cathedral Visitor.

The Bishop of Bristol, First Floor Hillside House, 1500 Parkway North, Stoke Gifford, Bristol BS34 8YU.

Telephone: 0117 906 0100

31. Complaints can also be made directly to the Information Commissioner's Office – www.ico.org.uk or telephone 0303 123 1113

Annex A: Key Definitions

data subject	the living individual about whom the data relates and who can be identified note – deceased persons are not covered by the regulation
data processing	Processing includes – obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, matching, transmitting, disseminating, making available, aligning, combining, blocking, erasing, destroying.
data controller	Bristol Cathedral – meaning the corporate body of Bristol Cathedral (HMRC Charity Reference number 567574886), Bristol Cathedral Enterprises Ltd (company registration number 02579801, Bristol Cathedral Trust (Charity Commission number 801008), the Friends of Bristol Cathedral (Charity Commission number 274399). the Dean (senior Priest) and Chapter are the Cathedral's governing body. See bristol-cathedral.co.uk for more information).
data processor	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller
personal data	means any information relating to an identified or identifiable natural person (data subject). Identifiers can include; name, number, location data, online identifier, or factors including physical, genetic, economic, cultural or social identity
third party	a natural or legal person, public authority, agency, body or company other than the data subject, controller and processor who may have access to personal data, or be authorised to process personal data
sensitive personal data	means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information and information concerning a person's health, sex life or sexual orientation