Archdiocese of Southwark

Data Protection (GDPR) Guidance

March 2019

Contents

Data Protection Policy for the Archdiocese of Southwark 4
1 Introduction and Background 4
2 The Data Protection Principles 4
3 The Diocesan Data Protection Officer and Registration with the ICO 5
4 How the Diocese will Comply and Demonstrate Compliance 5
5 Data Security & Responsibilities of Clergy, Staff and Volunteers 6
6 Privacy Notice 7
7 Processing, Disclosure and Sharing of Information 7
8 Fundraising and Marketing 10
9 Monitoring and Review 10
10 Contacts 10
11 Other Information Governance Policies 11
12 Glossary 11
Computer Usage Policy for The Roman Catholic Archdiocese Of Southwark (the "Diocese") 12
13 About this Policy 12
14 Personnel Responsible For The Policy 12
15 Equipment Security and Passwords 12
16 Systems and Data Security 13
17 Email 13
18 Using the Internet 14
19 Monitoring 16
20 Prohibited Use of Our Systems 16
21 Working Away from the Parish 16
IT Security Policy archdiocese of Southwark 17
22 About this Policy 17
23 Personnel Responsible For The Policy 17
24 Equipment Security and Passwords 17
25 Systems and Data Security 18
26 Email 18
27 Using the Internet 19
28 Personal Use of Our Systems 20
29 Monitoring 20
30 Prohibited Use of Our Systems 21

Bring Your Own Device Policy 22
31 Introduction 22
32 Data Protection and BYOD 22
33 The Responsibilities of Staff, Clergy and Volunteers 22
34 Monitoring and Access 24
Data Breach Procedure for the Archdiocese of Southwark 25
35 About this policy 25
36 Actions to take once an incident has been identified 25
37 Taking remedial action 26
38 Notifying a Personal Data breach 27
39 Follow-up action 27
40 Central logging of the issue 27
41 Glossary 28
Personal Data Breach Form For Archdiocese of Southwark 29
Part 1 29
part 2 30
Privacy Notice For Employees Archdiocese Of Southwark 33
58 About This Document 33
59 Details About Us 33
60 Personal Data We May Collect and Process 33
61 Sensitive Person Data Etc 34
62 Disclosure And Sharing Of Personal Information 34
63 Data Protection Principles – Our Obligations 35
64 Your Rights as a Data Subject 36

DATA PROTECTION POLICY FOR THE ARCHDIOCESE OF SOUTHWARK

1 INTRODUCTION AND BACKGROUND

1.1 The Archdiocese of Southwark (the "**Diocese**"), through its Trustees, is a Data Controller and consequently must process all Personal Data (including Special Categories of Personal Data) about Data Subjects in accordance with the General Data Protection Regulation 2016/679 (the "**GDPR**") and any other relevant data protection legislation, domestic or otherwise, (as may be in force or repealed or replaced from time to time) (together the "**Data Protection Rules**"). For the avoidance of doubt, the Diocese remains the sole Data Controller, even where Processing is carried out by its curial offices, parishes, departments and agencies. Please be aware that parishes form part of the Diocese and are not separate legal entities. Parishes are not Data Controllers, nor do they process Personal Data on behalf of the Diocese as a Data Processor.

1.2 The Diocese will collect, store, use and otherwise process Personal Data about the people with whom it interacts, who are the Data Subjects. This may include parishioners, volunteers, clergy, employees, contractors, suppliers and other third parties.

1.3 The Diocese processes Personal Data so that it can comply with its statutory obligations and achieve its charitable objects of advancing and maintaining the Roman Catholic religion through the operation of its parishes and its other activities.

1.4 Every Data Subject has a number of rights in relation to how the Diocese processes their Personal Data. The Diocese is committed to ensuring that it processes Personal Data properly and securely in accordance with the Data Protection Rules, as such commitment constitutes good governance and is important for achieving and maintaining the trust and confidence of Data Subjects. Therefore, the Diocese will regularly review its procedures to ensure that they are adequate and up-to-date.

1.5 All clergy, staff and volunteers of the Diocese who are involved in the Processing of Personal Data held by the Diocese have a duty to protect the data that they process and must comply with this Policy. The Diocese will take any failure to comply with this Policy or the Data Protection Rules very seriously. Any such failure may result in legal action being taken against the Diocese or the individual responsible.

2 THE DATA PROTECTION PRINCIPLES

2.1 The Diocese as the Data Controller is required to comply with the six data protection principles set out in the GDPR, which provide that Personal Data must be:

2.1.1 Processed fairly, lawfully and in a transparent manner;

2.1.2 Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes;

2.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

2.1.4 Accurate and, where necessary, kept up to date – every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay;

2.1.5 Kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed; and

2.1.6 Processed in a way that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational security measures.

2.2 There is also an overarching principle; the Data Controller must be able to demonstrate compliance with the six principles. Accountability is vital.

3 THE DIOCESAN DATA PROTECTION OFFICER AND REGISTRATION WITH THE ICO

3.1 The Diocesan Trustees have overall responsibility for compliance with the Data Protection Rules. However, the diocesan Data Protection Officer (the "**DPO**") shall be responsible for ensuring day-to-day compliance with this Policy and with the Data Protection Rules. The DPO will undergo training at least once every 12 months and the Diocese will provide the DPO with sufficient resources and support to carry out their responsibilities. The DPO's name and contact details can be found in section 10 of this Policy.

3.2 The Compliance Officer in the Finance Office will support the DPO with the day-to-day operation of the Data Protection regulations. Each Parish Priest, Dean and Agency Head will have responsibility for data protection within their own area.

3.3 The Diocese is registered with the Information Commissioner's Office (the "ICO") as a Data Controller, as is required by law. The Diocese will be responsible for paying to the ICO any future fees levied on Data Controllers by the Data Protection Rules.

3.4 This Policy applies to all Personal Data processed by the Diocese in whatever format (e.g. paper, electronic, film) and regardless of how it is stored (e.g. electronically or in filing cabinets). It also includes information that is in paper form but is intended to be put into electronic form and to any recordings made such as telephone recordings and CCTV.

4 HOW THE DIOCESE WILL COMPLY AND DEMONSTRATE COMPLIANCE

4.1 This Policy is intended to ensure that any Processing of Personal Data is in accordance with the Data Protection Rules and the data protection principles. The Diocese will therefore:

4.1.1 Ensure that, when personal information is collected (whether direct from the individual or from a third party), the Data Subject is provided with a Privacy Notice and informed of what data is being collected and for what legitimate purpose(s);

4.1.2 Be transparent and fair in processing Personal Data;

4.1.3 Take steps to ensure the accuracy of data at the point of collection and at regular intervals thereafter, including advising Data Subjects of their right to ask for rectification of Personal Data held about them;

4.1.4 Securely dispose of inaccurate or out-of-date data, or data which is no longer required for the purpose(s) for which it was collected;

4.1.5 Share information with others only when it is lawful to do so and ensure that individuals are informed of the categories of recipient to whom data will or may be disclosed and the purposes of any such disclosures;

4.1.6 Ensure that additional safeguards (as required by the Data Protection Rules) are in place to protect Personal Data that is transferred outside of the European Economic Area (the "**EEA**") (see section 7.4 of this Policy);

4.1.7 Ensure that data is processed in line with the Data Subject's rights, which include the right to:

(a) Request access to Personal Data held about them by the Diocese (including, in some cases, having it provided to them in a commonly used and machine-readable format);

(b) Have inaccurate Personal Data rectified;

(c) Have the processing of their Personal Data restricted in certain circumstances;

(d) Have Personal Data erased in certain specified situations (in essence where the continued processing of it does not comply with the Data Protection Rules);

(e) Prevent the processing of Personal Data for direct-marketing purposes (which includes for fundraising and wealth screening purposes);

(f) Ask the Diocese to prevent Processing of Personal Data which is likely to cause unwarranted or substantial damage or distress to the Data Subject or any other individual; and

(g) Prevent, in some cases, decisions being made about them which are based solely on automated processing (i.e. without human intervention) and which produce significant or legal effects on them;

4.1.8 Ensure that all clergy, volunteers and employees are aware of and understand the Diocese's data protection policies and procedures; and

4.1.9 The Diocese has 2 retention schedules – one issued by the Diocesan Archives covering parish records and one issued by the Finance Office covering' business' and other records. These set out the periods for which different categories of Personal Data should be kept and MUST be used.

4.2 Through adherence to this Policy and related data protection policies, and through appropriate record-keeping, the Diocese will seek to demonstrate compliance with each of the data protection principles. All data protection documentation is available on the diocesan website and will be updated as necessary.

4.3 In addition, the Data Protection Rules require the Data Controller to carry out a Data Protection Impact Assessment (a "**DPIA**") prior to undertaking any Processing of Personal Data that is "likely to result in a high risk for the rights and freedoms" of individuals. DPIAs will therefore be considered where appropriate in relation to the implementation of any new projects, services or systems which could result in a high privacy risk to individuals (particularly where new technology is being deployed). Please contact the DPO for guidance (see section 10 of this Policy).

5 DATA SECURITY & RESPONSIBILITIES OF CLERGY, STAFF AND VOLUNTEERS

5.1 The Diocese must ensure that appropriate technical and organisational security measures are in place to prevent unauthorised or unlawful Processing or damage to or loss (accidental or otherwise), theft, or unauthorised disclosure of Personal Data (a "Data Breach"). In particular, all clergy, employees and volunteers should ensure that:

5.1.1 The only individuals who have access to Personal Data and are able to process it are those who are authorised to do so;

5.1.2 Personal Data **may not** be stored on individual PCs, portable electronic devices or removable storage media but can only be stored on centrally accessed Diocesan networks and properly encrypted parish/agency hardware. Only encryption approved by Diocesan IT will be deemed to meet the required encryption standards. Individual devices can be used as portals to personal data held on diocesan systems;

5.1.3 Passwords are kept confidential, are changed regularly and are not shared between individuals;

5.1.4 PCs are locked or logged off and paper documents are securely locked away when individuals are away from their desks;

5.1.5 Offices, desks and filing cabinets/cupboards are kept locked if they contain Personal Data of any kind, whether in digital or electronic format or on paper;

5.1.6 When destroying Personal Data, paper documents are securely shredded, and electronic data is securely deleted; and

5.1.7 Personal Data removed from an office is subject to appropriate security measures, including keeping paper files in a place where they are not visible or accessible by the public; using passwords/passcodes; encrypting portable electronic devices and storing such devices securely (e.g. not left in the boot of a car overnight).

5.2 In the event that you become aware that there has been a Data Breach, or you suspect there might have been, you must report this immediately to the DPO following the Data Breach Procedure at dpo@rcaos.org.uk. Further contact details for the DPO can be found in section 10 of this Policy.

6 PRIVACY NOTICE

6.1 When any Personal Data is collected from an individual, they must be provided with a Privacy Notice. The Privacy Notice provides information about what, why and how information is processed. Privacy Notices are available on the diocesan website.

7 PROCESSING, DISCLOSURE AND SHARING OF INFORMATION

The Diocese processes personal data for a number of different purposes, including:

Lawful Ground for Processing of Personal Data	**Examples**
Where we have an individual's consent	• Posting photographs of an individual on a diocesan website • Before any announcements that someone is sick • Sending individuals marketing or fundraising communication by email or SMS
Where it is necessary for the performance of a contract to which an individual is party	• Where an individual enters into a hiring agreement for one of our facilities
Where it is necessary for compliance with a legal obligation	• Passing on information to a local authority or the Charity Commission • Passing Gift Aid information to HMRC
Where it is necessary to protect the vital interests of an individual	• Passing on information to the Police • Passing on information about an individual's serious health condition to the NHS or a health professional where

	there is a risk of death or serious injury to that person or another individual
Where it is necessary for performance of a task in the public interest	• Updating and maintaining the register of marriages
Where is it necessary for the purposes of the legitimate interests pursued by the Diocese or a third party	• Using baptism data to follow up with families for first communion

Lawful Ground for Processing of Special Categories of Data	**Examples**
Where we have an individual's explicit consent	• To cater for an individual's dietary or medical needs at an event
Where it is necessary for compliance with a legal obligation	• Passing on information to the local authority
Where it is necessary to protect the vital interests of an individual	• Passing on information to the Police • Passing on information about an individual's serious health condition to the NHS or a health professional where there is a risk of death or serious injury to that person or another individual
Where it is carried out in the course of the Diocese's legitimate activities by a not-for-profit body with religious aims	• Carrying out a parish census
Where information has manifestly been made public	• Referring to a public figure who is well known as a member of the church, as a Catholic
Where we are establishing, exercising or defending legal claims	• Providing information to our insurers or lawyers in connection with legal proceedings
Where the processing is for reasons of substantial public interest	• Where steps are taken to prevent fraud or other dishonest activity
Where the processing is necessary for archiving historical records	• Maintenance of parish records

7.1 DISCLOSING PERSONAL DATA

7.1.1 When receiving telephone or email enquiries, clergy, employees and volunteers should exercise caution before disclosing any Personal Data. The following steps should be followed:

(a) Ensure the identity of the person making the enquiry is verified and check whether they are entitled to receive the requested information;

(b) Require the enquirer to put their request in writing so that their identity and entitlement to receive the information can be verified if the information is particularly sensitive and/or you are not confident the person is entitled to the information;

(c) If there is any doubt, refer the request to the DPO for assistance (particularly where Special Categories of Personal Data are involved); and

(d) When providing information, ensure that Personal Data is securely packaged and sent by the most appropriate means (e.g. special delivery, courier or hand

delivery) in accordance with the Data Protection Rules, the Privacy Notice and this Policy.

7.1.2 Please remember that parents and guardians are only entitled to access information about their child if the child is unable to act on their own behalf (e.g. because the child is not mature enough to understand their rights) or if the child has given their consent. If you are unsure about whether or not to provide information about a child to a parent or guardian, please speak to the DPO before providing any information. Children from 12 years upwards are generally to be taken as being capable of understanding their rights and making decision regarding their own information. However, consideration of the particular circumstances and the child's capacity must be given in each circumstance.

7.1.3 **Please also remember that individuals are only entitled to obtain information about themselves** and not any other third parties (e.g. a family member, other parishioner or member of clergy or staff).

7.2 DATA PROCESSORS

7.2.1 The Diocese may instruct another body or organisation to process Personal Data on its behalf as a Data Processor (e.g. a payroll provider, a third-party IT provider). In such situations, the Diocese will share necessary information with the Data Processor but will remain responsible for compliance with the Data Protection Rules as the Data Controller.

7.2.2 Personal Data will only be transferred to a third-party Data Processor if the DPO is satisfied that the third party has in place adequate policies and procedures to ensure compliance with the Data Protection Rules. There should also be a written contract in place between the Diocese and the Data Processor, which includes provisions to ensure that the Data Processor complies with the requirements of the Data Protection Rules. If you have authority to enter into contracts, please refer to the Data Processor Contract Checklist.

7.3 THIRD PARTY REQUESTS

7.3.1 The Diocese may from time to time receive requests from third parties for access to documents containing Personal Data. The Diocese may disclose such documents to any third party where it is legally required or permitted to do so. Such third parties may include health professionals, the Police and other law enforcement agencies, the Charity Commission, HMRC, other regulators, immigration authorities, insurers, local authorities (e.g. Trading Standards), Courts and Tribunals or organisations seeking references.

7.3.2 Anyone in receipt of any verbal or written request from any person for access to, or disclosure of, any Personal Data outside of normal Diocesan operations must immediately contact the DPO.

7.4 TRANSFERS OF PERSONAL DATA OUTSIDE OF THE EEA

7.4.1 The Data Protection Rules require Data Controllers to put additional safeguards in place when transferring Personal Data outside of the EEA (e.g. to the Vatican). Additionally, such transfers can only take place on a number of legal grounds. The Diocese does not generally store Personal Data outside of the UK. However, the Diocese may transfer Personal Data outside of the EEA either where requested by the Data Subject (e.g. marriage record) or where necessary (e.g. a student studying abroad), on the basis of the Data Subject's informed consent. The DPO may also authorise transfers where another legal ground in the Data Protection Rules is met.

7.5 SUBJECT ACCESS REQUESTS (SARs)

7.5.1 Any Data Subject may exercise their rights as set out above (e.g. the right of access to the Personal Data which the Diocese holds about them, or the right to have Personal Data erased). Any and all such requests should immediately be referred to the DPO.

7.5.2 To be valid, a Subject Access Request must be made in writing (including requests made via email or on social media) and provide enough information to enable the Diocese to identify the Data Subject and to comply with the request.

7.5.3 All Subject Access Requests will be dealt with by the DPO. Clergy, employees or volunteers who receive a Subject Access Request (or anything they suspect could be a SAR) must forward it to the DPO immediately in order that such requests can be replied to within the strict deadlines set out in the Data Protection Rules (generally one month from the date of the request).

7.5.4 No fees will be charged for dealing with Subject Access Requests unless a request is considered to be manifestly unfounded, excessive or repetitive. Fees may be charged to provide additional copies of information previously provided. Where the Diocese considers a request to be manifestly unfounded, excessive or repetitive, the Diocese may lawfully refuse to respond and, if so, the DPO will inform the Data Subject of this in writing within the one-month period.

8 FUNDRAISING AND MARKETING

8.1 Any use of Personal Data for marketing (including fundraising) purposes must comply with the Data Protection Rules and the Privacy and Electronic Communications Regulations (the "PECR") (and any replacement legislation), which relate to marketing by electronic means.

8.2 Individuals have a right to object to their Personal Data being used for electronic marketing purposes. Individuals must be informed of their right to object when their data is collected. If an objection is received, no further marketing or fundraising communications must be sent to them.

8.3 The PECR requires that the Diocese has the prior consent of recipients in certain circumstances before it sends any unsolicited electronic messages for the purpose of fundraising, or other marketing activities (e.g. events).

9 MONITORING AND REVIEW

9.1 This policy will be reviewed every 12 months and may be subject to change.

10 CONTACTS

10.1 Any queries regarding this Policy should be addressed to the Diocesan Data Protection Officer, Sarah Williams, who can be contacted by email at dpo@rcaos.org.uk, by telephone 020 7960 2500 or at the following address:

Data Protection Officer

RC Archdiocese of Southwark

Finance Office

59 Westminster Bridge Road

London SE1 7JE

10.2 Complaints will be dealt with in accordance with the Diocesan Complaints Policy.

10.3 Further advice and information can be obtained from the Information Commissioner's Office at www.ico.org.uk

11 OTHER INFORMATION GOVERNANCE POLICIES

11.1 This Policy must be read in conjunction with:

11.1.1 The Diocesan Privacy Notice

11.1.2 The Diocesan Complaints Policy

11.1.3 The Diocesan Computer Usage Policy (see below)

These policies are available on the diocesan website **www.rcsouthwark.co.uk**.

12 GLOSSARY

"**Data Controller**" means a person, organisation or body that determines the purposes for which, and the manner in which, any Personal Data is processed. A Data Controller is responsible for complying with the Data Protection Rules and establishing practices and policies in line with them.

"**Data Processor**" means any person, organisation or body that Processes personal data on behalf of and on the instruction of the Diocese. Data Processors have a duty to protect the information they process by following the Data Protection Rules.

"**Data Subject**" means a living individual about whom the Diocese processes Personal Data and who can be identified from the Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data and the information that the Diocese holds about them.

"**Personal Data**" means any information relating to a living individual who can be identified from that information or in conjunction with other information which is in, or is likely to come into, the Diocese's possession. Personal Data can be factual (such as a name, address or date of birth) or it can be an opinion (e.g. a performance appraisal). It can even include a simple email address. A mere mention of someone's name in a document does not necessarily constitute Personal Data, but personal details such as someone's contact details or salary (if it enabled an individual to be identified) would fall within the definition.

"**Processing**" means any activity that involves use of Personal Data. It includes obtaining, recording or holding the information or carrying out any operation or set of operations on it, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring or disclosing Personal Data to third parties.

"Special Categories of Personal Data" (previously called sensitive personal data) means information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexuality. It also includes genetic and biometric data. Special Categories of Personal Data can only be processed under strict conditions and such processing will usually, although not always, require the explicit consent of the Data Subject.

COMPUTER USAGE POLICY FOR THE ROMAN CATHOLIC ARCHDIOCESE OF SOUTHWARK (THE "DIOCESE")

13 ABOUT THIS POLICY

13.1 This policy is designed to detail how computer systems within the Diocese must be used. It covers anyone (clergy, employees, volunteers, workers, etc.) who has access to Diocesan computer systems. Failure to adhere to this policy will be treated extremely seriously and could, in the case of employees, lead to disciplinary action.

14 PERSONNEL RESPONSIBLE FOR THE POLICY

14.1 This policy has been written by the diocesan Finance Office. It will be updated from time to time or as legislation changes. At a local level the parish priest or agency head has responsibility for ensuring that the policy is properly implemented and adhered to.

15 EQUIPMENT SECURITY AND PASSWORDS

15.1 All systems MUST be password protected. Each user of the system MUST have their own password and passwords must never be shared. You may be required to have different passwords for access to different accounts. Passwords MUST be strong and contain at least 8 characters and be a mix of upper and lower letters, numbers and characters. Passwords MUST be changed once a month.

15.2 Please remember that the data held on diocesan devices is the responsibility of the data controller and access cannot be denied to the Diocese, by the usual user. Failure to provide access if requested will lead to disciplinary action and possibly legal action.

15.3 A central repository of passwords will be retained by ICT Support in case a device needs to be accessed, for example due to absence of the user or corruption of the data.

15.4 Personal diocesan data MUST NOT be held on personally owned devices (PC, laptop, mobile phone, etc). Personally, owned devices can be used as a portal to access personal data held, for example, in the cloud, but it MUST NOT be stored on the device. If the action of accessing documents via the cloud automatically downloads them to the device, they MUST BE deleted from the device. If your personal device automatically downloads or syncs diocesan emails, this function MUST be disabled. Personal devices can be used to access diocesan emails provided that it is done via a portal. If you have personal data stored on your own device and that device is lost or stolen it would constitute a breach under the GDPR.

15.5 If you have a diocesan mobile device, it MUST be encrypted to current (January 2019) standards. Please contact **ICTSUPPORT@finance-rcdsouthwark.org** to check any devices you may have.

15.6 Parish/agency desktops will also need to have current encryption. Please contact **ICTSUPPORT@finance-rcdsouthwark.org** or visit our website to ensure that you have the most up-to-date encryption.

15.7 All parish/agency devices MUST have the most up-to-date antivirus software. Please contact **ICTSUPPORT@finance-rcdsouthwark.org** or visit our website to ensure that you have the most up-to-date version.

16 SYSTEMS AND DATA SECURITY

16.1 Threats to cyber security are rife and it is the most commonly exploited area for crime such as ID thefts and banking/payment fraud. Criminal access to data is achieved in a variety of ways including fake emails, emails or attachments containing viruses and users being tricked into revealing data. This means that we all have to be extra vigilant in how we manage our IT activity. NEVER open an email or attachment that looks suspicious or click on a link that you don't know what it is. Suspicious emails might be identified by unusual formatting/fonts or strange wording in the subject line or sender. Please delete any such emails without opening them. Only open attachments or click on links if you know where they have come from.

16.2 The Diocese has the right to block certain content and/or access to certain websites and users should not attempt to access blocked content or password protected areas.

16.3 You MUST NEVER load software on to Diocesan systems without the express permission of ICT Support.

16.4 If you think you may have accidentally introduced a virus into a diocesan system, please contact ICT Support immediately.

16.5 All systems should be regularly backed up. It is recommended that each parish/agency backs up their own system daily to an encrypted (to current standards) external drive, which is then stored in a safe. If you need help with this, please contact **ICTsupport@finance-rcdsouthwark.org**.

17 EMAIL

17.1 Our email code of conduct has been put in place to ensure the appropriate use of the system. The code covers all diocesan email users in the following circumstances: -

17.1.1 E-mail technology used on behalf of the Diocese, its parishes and agencies and any other associated organisations

17.1.2 E-mail technology used on hardware and/or software provided by the Diocese its parishes and agencies and any other associated organisations

17.1.3 The technology used to communicate information about the Diocese and associated organisations and people

17.1.4 The technology used to communicate any information that has been gained from the Diocese its parishes and agencies and any other associated organisations

17.1.5 The email system provided by the Diocese is for Diocesan business use and can be accessed by the Diocese. If you use it for personal use you do so at your own risk and accept that those emails are also accessible by the Diocese. If you do not wish any personal emails to be accessed DO NOT use your Diocesan email address for personal use.

The rules of the Code are as follows: -

17.2 Bullying, harassment or abuse of others through the use of email is forbidden. This includes sending information that insults or harasses others with respect to gender/gender reassignment, religion/belief, ethnic/national origin, age, sexual orientation, martial/civil partnership status, pregnancy/maternity or disability. If anyone feels that they have been bullied or harassed via email, please raise your concerns with the HR Manager in the first instance.

17.3 It is expressly forbidden to: -

- Access or distribute illegal images
- Access or distribute pornography
- Engage in on line gambling

- Take part in electronic chain letters or other types of messaging
- Send or forward junk email
- Run a business
- Download or distribute copyright information
- Download, open or distribute unauthorised software
- Post confidential information about the Diocese or any related parties without authorisation.
- Send data belonging to the Diocese to a home computer or other personal device

17.4 When replying to an email, make sure that the reply is for the sender only and not original mailing list (unless there is a requirement to do so).

17.5 When attaching files to a message, keep them small and ensure that they are PASSWORD PROTECTED if they contain personal data. Email is not the medium to use for very high resolution graphics. In addition, do not attach files that have hidden confidential information. Software exists that can reveal this hidden data.

17.6 Remember: -

- Emails can be read by third parties (police can obtain printouts directly from internet service providers without a warrant).
- Email can be used in evidence.
- Email can create binding contracts.
- Email may contain content which is subject to the Data Protection Act
- Make sure that the content of your email is factually correct and non-defamatory.
- Emails have to be disclosed in certain legal proceedings

17.7 It is forbidden to send email using a mail client (i.e. software) that has been installed for another employee (i.e. someone else will appear to be the sender.). In addition, employees must take adequate precautions to prevent this (e.g. ensure that PC's are not left switched on and unattended for long periods of time).

17.8 An individual's PC may be audited at any time to ensure compliance to the code of conduct.

17.9 Please ensure your Email has the approved **Diocesan Signature and Disclaimer** at the bottom of all sent Emails. The current wording is:

Name
Role Title
Parish/Agency Name and Address
Parish/Agency Telephone Number

This message is only for the use of the intended recipient(s). It may contain information which is confidential and legally privileged within the meaning of applicable law. If you are not the intended recipient, please contact the sender as soon as possible. Any copying, disclosure, distribution or any action taken or omitted to be taken in reliance on it is prohibited and may be unlawful. Unless stated to the contrary, any opinions expressed in this message are personal and may not be attributed to the Roman Catholic Archdiocese of Southwark.

18 USING THE INTERNET

18.1 The Diocese has a Social Media Policy which MUST be observed at all times. The policy is available on the diocesan website

http://www.rcsouthwark.co.uk/media/Social%20Media%20Policy%20-%20Approved%20version%20-%2017%20M11.pdf

18.2 Access to the Internet is provided for business use. **Reasonable personal use is permitted, but this must not be abused. Abuse of the system will lead to disciplinary action and may result in access to the Internet being denied to all users. It may also be reported to the police.**

18.3 The Diocese assumes no liability for loss, damage, destruction, alteration, disclosure, or misuse of any personal data or communications transmitted or stored using its computers, computer networks, or on-line accounts for personal use. Moreover, the Diocese accepts no responsibility or liability for the loss or non-delivery of any personal e-mail communication.

18.4 Access to social networking sites – e.g. Facebook, Twitter, LinkedIn, etc. is not generally required as part of the business of the Diocese. Where it is part of Diocesan business – e.g. a parish Facebook page, only the diocesan social media account should be accessed through diocesan devices. Networking sites MUST NOT be left open whilst other work is undertaken as constant feeds are distracting and may permit unauthorised access.

18.5 The creation, generation and distribution of material through social media that is offensive on the grounds of gender/gender reassignment, religion/belief, ethnic/national origin, age, sexual orientation, martial/civil partnership status, pregnancy/maternity or disability is forbidden. Please remember that under current legislation complaints can be made by anyone who finds the material offensive whether or not it was directed at them personally.

18.6 It is forbidden to use the internet to generate and/or distribute material which is offensive to, or ridicules other employees or anyone else associated with the Diocese.

18.7 The use of Diocesan technology to access, store or distribute of any kind of offensive material (including all pornography) is expressly forbidden. It may also be illegal and lead to prosecutions of both the employee and the Diocese.

18.8 Any illegal activity will be reported to the police.

18.9 In these rules, material will be considered offensive if it causes distress to the person who receives it, discovers it and/or if it is defined as illegal under current legislation. Please remember that under current legislation complaints can be made by anyone who finds the material offensive whether or not it was directed at them personally.

18.10 Accidental sending or receiving of such material will not be an acceptable excuse.

18.11 The Diocese considers any breach of these rules to be serious and will automatically invoke the Disciplinary Procedure. Depending upon the nature of the breach, it could be considered as Gross Misconduct and/or involve reporting to the Police. The Diocese reserves the right to use monitoring software as it sees fit.

18.12 The following websites are specifically excluded from access at the Diocese:

- adult/sexually explicit
- gambling
- violence
- drugs and alcohol
- hacking
- remote proxies
- chat
- personals and dating

18.13 Parishes/agencies MUST be in a position to block such websites. They should be using the Diocesan recommended anti-virus application which will enable this to happen. Contact the ICTsupport@finance-rcdsouthwark.org for more information.

19 MONITORING

19.1 Like most organisations, the Diocese has the technical capability to monitor activity on its systems and reserves the right to do so. This will not be used on a regular basis but will only be used in exceptional circumstances and/or to retrieve any lost data/history.

20 PROHIBITED USE OF OUR SYSTEMS

20.1 The Diocese takes the misuse of its systems very seriously. Failure to comply with this policy will lead to disciplinary action, which could include dismissal and may result in the involvement of the police. If banned activity is discovered remote technical steps will be taken to secure evidence and prevent further misuse.

21 WORKING AWAY FROM THE PARISH

21.1 With express permission of your parish priest, in your capacity as a parish volunteer, you may take materials away from the parish to be worked on, subject to the following:

- You inform the Parish Priest what materials you are taking with you
- When you will be returning those materials back to the parish
- You must take care of the materials and guard them against theft or loss as these may contain personal or sensitive data
- The materials that you take are stored safely when you are not working with them
- If you are using your own electronic equipment, you must not download any content onto your devices
- Any documents/spreadsheets relating to the materials from the parish and is on your electronic device remains the property of the Parish and must be deleted when you have completed the task you are undertaking
- Any electronic data that you create off-site must be subject to password protection, for example, creating a spreadsheet of names and addresses from paper documents

IT SECURITY POLICY ARCHDIOCESE OF SOUTHWARK

22 ABOUT THIS POLICY

22.1 Our IT and communications systems are intended to promote effective communication and working practices within our organisation. This Policy outlines the standards you must observe when using these systems, the circumstances in which we will monitor your use, and the action we will take in respect of breaches of these standards.

22.2 This Policy covers all trustees of the Diocese, officers, consultants, contractors, volunteers, casual workers, agency workers, parishioners, members and anyone who has access to our IT and communication systems.

22.3 Misuse of IT and communications systems can damage the Archdiocese and our reputation as well as causing harm and distress to any affected individuals. Breach of this Policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal or removal from your post.

22.4 This policy does not form part of any contract between you and the Archdiocese and we may amend it at any time.

23 PERSONNEL RESPONSIBLE FOR THE POLICY

23.1 The trustees have overall responsibility for the effective operation of this Policy and for ensuring compliance with the relevant statutory framework. All employees are responsible for ensuring that they comply with this policy.

23.2 All individuals who work for the Archdiocese have a specific responsibility to ensure the fair application of this Policy and all individuals who work for or are members of the Archdiocese are responsible for supporting colleagues and ensuring its success.

23.3 The Finance Department will deal with requests for permission or assistance under any provisions of this Policy and may specify certain standards of equipment or procedures to ensure security and compatibility. Upon request for assistance, a member of the Finance Department will contact the Diocesan External IT provider if appropriate.

24 EQUIPMENT SECURITY AND PASSWORDS

24.1 You are responsible for the security of the equipment allocated to or used by you and must not allow it to be used by anyone other than in accordance with this Policy.

24.2 You are responsible for the security of any computer device used by you. You should lock your device or log off when leaving it unattended or on leaving the office, to prevent unauthorised users accessing the system in your absence. Anyone who is not authorised to access our network should only be allowed to use devices under supervision.

24.3 Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first informing a member of the Finance Department who will consult with the external IT providers. You should use passwords on all IT equipment, particularly items that you take out of the office. You must keep your passwords confidential and change them regularly. You must not use another person's username and password or make available or allow anyone else to log on using your username and password unless authorised by your head of department or line manager. On the termination of your work for the Archdiocese (for any reason) you must provide details of your

passwords to the Financial Secretary, or person nominated by her and return any equipment, key fobs or cards.

24.4 If you have been issued with a laptop, tablet computer, BlackBerry, smartphone or other mobile device, you must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. You should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

25 SYSTEMS AND DATA SECURITY

25.1 You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

25.2 You must not download or install software from external sources without authorisation from your head of department, or external IT provider as appropriate. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked by the Diocesan IT provider before they are downloaded. If in doubt, staff should seek advice from your head of department or line manager. You must not attach any device or equipment to our systems without authorisation from the external IT provider. This includes any USB flash drive, MP3 player, tablet, smartphone or other similar device, whether connected via the USB port, infra-red connection or in any other way.

25.3 We monitor all emails passing through our system for viruses. You should exercise particular caution when opening unsolicited emails from unknown sources or an email which appears suspicious (for example, if it contains a file whose name ends in .exe). Inform your head of department, the Financial Secretary and ensure that the external IT provider has been notified immediately if you suspect your computer may have a virus or if you have opened any suspicious email attachments or clicked on any suspicious links. We reserve the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.

25.4 You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your duties.

25.5 You must be particularly vigilant if you use our IT equipment outside the workplace and take such precautions as we may require from time to time against importing viruses or compromising system security. The system contains information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

26 EMAIL

26.1 Although email is a vital business tool, you should always consider if it is the appropriate method for a particular communication. Correspondence with third parties by email should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals.

26.2 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails. Anyone who feels that they are being or have been harassed or bullied or is offended by material received from a colleague via email, should inform their line manager and Financial Secretary immediately.

26.3 You should take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Remember that you have no control over where your email may be forwarded by the

recipient. Avoid saying anything which would cause offence or embarrassment if it was forwarded to colleagues or third parties or found its way into the public domain.

26.4 Email messages are required to be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

26.5 In general, you should not:

26.5.1 send, forward or read private emails at work which you would not want a third party to read;

26.5.2 send or forward chain mail, junk mail, cartoons, jokes or gossip;

26.5.3 contribute to system congestion by sending trivial messages, copying or forwarding emails to those who do not have a real need to receive them, or using "reply all" unnecessarily on an email with a large distribution list;

26.5.4 sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals;

26.5.5 agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter;

26.5.6 download or email text, music or any other content on the internet which is subject to copyright protection, unless it is clear that the owner of such works allows this;

26.5.7 send messages from another person's email address (unless authorised) or under an assumed name; and/or

26.5.8 send confidential messages via email or the internet, or by other means of external communication which are known not to be secure.

26.6 If you receive an email in error you should inform the sender. If you have sent an email in error contact your head of department and the Data Protection Officer immediately.

26.7 Do not use your own personal email account to send or receive email for the purposes of our business. Only use the email account we have provided for you.

27.8 We do not permit access to web-based personal email such as Gmail or Hotmail or document storage applications such as Dropbox on our computer systems at any time due to additional security risks.

27 USING THE INTERNET

27.1 Internet access is provided primarily for business purposes. Occasional personal use may be permitted as set out in paragraph 7.

27.2 When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in paragraph 9.1, such a marker could be a source of embarrassment to the visitor and us, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature.

27.3 You should not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral. Even web content which is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this Policy.

27.4 Except as authorised in the proper performance of your duties, you should not under any circumstances use our systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in your own time.

27.5 The following must never be accessed from our network: online radio, audio and video streaming, instant messaging, webmail such as Gmail or Hotmail, document storage applications such as Dropbox and social networking sites (including, but not limited to, Facebook, Twitter, YouTube, Google+, Instagram, SnapChat, Pinterest, Tumblr, Second Life. This list is non-exhaustive may be modified from time to time.

28 PERSONAL USE OF OUR SYSTEMS

28.1 We permit the incidental use of our internet, email and telephone systems to send personal email, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

28.2 Personal use must meet the following conditions:

28.2.1 use must be minimal and take place substantially out of normal working hours (that is, during lunch hours, before 9 am or after 5.30 pm);

28.2.2 personal emails should be labelled “personal” in the subject header;

28.2.3 use must not interfere with business or office commitments;

28.2.4 use must not commit us to any marginal costs; and

28.2.5 use must comply with this Policy (see in particular paragraph 5 and paragraph 6) and our other policies including our Data Protection Policy and Privacy Policy for Websites.

28.3 You should be aware that personal use of our systems may be monitored (see paragraph 8) and, where breaches of this Policy are found, action may be taken under the Disciplinary Procedure (see paragraph 9). We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

29 MONITORING

29.1 Our systems enable us to monitor telephone, email, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

29.2 A CCTV system monitors the exterior of the building 24 hours a day. This data is recorded.

29.3 We reserve the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

29.3.1 to monitor whether use of the email system or the internet is legitimate and in accordance with this Policy;

29.3.2 to find lost messages or to retrieve messages lost due to computer failure;

29.3.3 to assist in the investigation of alleged wrongdoing; and

29.3.4 to comply with any legal obligation.

30 PROHIBITED USE OF OUR SYSTEMS

30.1 Misuse or excessive personal use of our telephone or email system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some circumstances be a criminal offence. In particular, it will usually amount to gross misconduct to misuse our systems by participating in online gambling, forwarding chain letters, or by creating, viewing, accessing, transmitting or downloading any of the following material (this list is not exhaustive):

30.1.1 pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

30.1.2 offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our parishioners;

30.1.3 a false and defamatory statement about any person or organisation;

30.1.4 material which is discriminatory, offensive, derogatory or may cause embarrassment to others;

30.1.5 confidential information about us, our work, or any of our workers, or parishioners (except as authorised in the proper performance of your duties);

30.1.6 any other statement which is likely to create any criminal or civil liability (for you or us); and/or

30.1.7 music or video files or other material in breach of copyright.

Any such action will be treated very seriously and is likely to result in summary dismissal or removal from your post.

30.2 Where evidence of misuse is found, we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.

BRING YOUR OWN DEVICE POLICY

31 INTRODUCTION

31.1 The Archdiocese recognises the benefits that can be achieved by allowing staff, clergy and volunteers to use their own electronic devices when working or undertaking their ministry or volunteering tasks for the Diocese or its parishes, whether that is at home, in the offices or on parish premises, or while travelling.

31.2 Such devices include laptops, smartphones and tablets, and the practice is commonly known as 'bring your own device' or BYOD. The Archdiocese is committed to supporting staff and volunteers in this practice and ensuring that as few technical restrictions as reasonably possible are imposed on those accessing systems and data using their own devices.

31.3 The use of personal devices to process data creates issues that need to be addressed, particularly regarding information security.

31.4 The Archdiocese, as a data controller, must ensure that it remains in control of all data for which it is responsible, regardless of the ownership of the device used to carry out the processing. It must also protect its intellectual property as well as empowering staff, clergy and volunteers to ensure that they protect their own personal information.

32 DATA PROTECTION AND BYOD

32.1 The Archdiocese must process personal data in accordance with the data protection laws. Special categories of personal data e.g. concerning race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation should be handled with a higher degree of protection at all times and always in accordance with the data protection laws and the Data Protection Policy.

32.2 The Archdiocese in line with guidance from the Information Commissioner's Office (ICO) on BYOD, recognises that there are inherent risks in using personal devices to hold personal data. Therefore staff, clergy and volunteers must follow the guidance in this Policy when considering taking advantage of any authorisation given to use a personal device to access Archdiocesan data. Permission must be obtained from your relevant line manager, before using your own device for work purposes.

32.3 A data loss or breach resulting from the careless loss or misuse of your own device could result in a substantial fine for the reputational damage.

32.4 Any member of staff found to have deliberately breached this Policy may be subject to disciplinary measures and could have access to the facilities withdrawn.

33 THE RESPONSIBILITIES OF STAFF, CLERGY AND VOLUNTEERS

33.1 Individuals who make use of the BYOD Policy must take responsibility for their own device, its content and how they use it. Therefore, you must:

33.1.1 familiarise yourself with your device and its security features so that you can ensure the safety of data (as well as your own information);

33.1.2 ensure that appropriate security features and measures are in place on the device;

33.1.3 maintain the device yourself ensuring that it is regularly patched and upgraded (only using operating systems, office suites and other software which are currently supported by their suppliers); and

33.1.4 ensure that the device is not used for any purpose that would conflict with the Computer systems and policies.

33.2 While IT staff will always endeavour to assist individuals wherever possible, the Archdiocese cannot take responsibility for supporting devices not provided by the Archdiocese.

33.3 If you are taking advantage of this Policy, you must take all reasonable steps to:

33.3.1 prevent theft and loss of Archdiocese data, or the device itself;

33.3.2 keep data confidential where appropriate;

33.3.3 maintain the integrity of data; and

33.3.4 take responsibility for any software that you download onto the device.

33.4 If you are using your own device under this Policy, you must you must also:

33.4.1 set up pass-phrases, passwords, passcodes, passkeys or biometric equivalents (as applicable). These must be of sufficient length and complexity for the particular type of device. If your device is used to access Archdiocese or parish emails, you must use a second, different password to log-in to the email account (this is called “double-locking”);

33.4.2 set up remote wipe facilities (if available) and implement a remote wipe if you lose the device or allow IT staff to do this on your behalf;

33.4.3 encrypt devices and content, as necessary;

33.4.4 not hold any information relating to Archdiocese business that is sensitive, personal, confidential or of commercial value on personally-owned devices. For the sake of clarity, this means that files, images etc that relate to Diocesan business should not be kept on the C drive or other hard-drive built into the device. Instead, you should use your device to make use of storage and working services on systems that the Archdiocese offers or recommends, allowing access to data securely over the internet;

33.4.5 where it is necessary for Archdiocese data to be held on a personal device, delete it as soon as possible once it is no longer required. This includes information contained within emails;

33.4.6 where appropriate, ensure that Archdiocese data is copied back onto the systems, and manage any potential data integrity issues with existing information (e.g. make sure you do not inadvertently wipe or copy over prior information or documents);

33.4.7 if data has to remain temporarily on a device, ensure that it is backed-up daily onto a secure external medium such as an encrypted memory stick – but this should not become normal practice;

33.4.8 report the loss of any device containing Archdiocese data or content to the Data Protection Officer and, where possible, IT support;

33.4.9 be aware of any data protection issues and ensure that personal data is handled appropriately;

33.4.10 report any security breach immediately to the DPO in accordance with the diocesan Data Protection Policy; and

33.4.11 ensure that no Archdiocese data is left on any personal device indefinitely. Particular care must be taken if a device is disposed of/sold/transferred to a third party to ensure that it is wiped. Ask IT support for more guidance.

34 MONITORING AND ACCESS

34.1 The Archdiocese will not routinely monitor personal devices. However, it does reserve the right to:

34.1.1 prevent access to a particular device from either the wired or wireless networks or both;

34.1.2 prevent access to a particular system; and

34.1.3 take all necessary and appropriate steps to retrieve Archdiocese data.

DATA BREACH PROCEDURE FOR THE ARCHDIOCESE OF SOUTHWARK

35 ABOUT THIS POLICY

35.1 This Policy describes the actions that must be taken by staff to report any incident which may result in a Personal Data breach. A "Personal Data breach" is defined in Article 4(12) of the General Data Protection Regulation (GDPR) as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

35.2 Often, when an incident first comes to light, it will not be possible to determine whether or not it constitutes a Personal Data breach. The term "incident" is used in this Policy to describe any situation which may, upon investigation, turn out to be a Personal Data breach.

35.3 This Policy should be read in conjunction with the Data Protection Policy which can be found in the Staff Handbook which has been circulated throughout the Curial Office and Parishes.

35.4 An incident may come to light in a number of ways. For example, it could occur by:

35.4.1 direct observation e.g. where a member of staff spots that Personal Data has been sent to the wrong email address;

35.4.2 being reported to us by a Data Subject: e.g. where a Data Subject notifies us that s/he has received Personal Data relating to another Data Subject;

35.4.3 being reported to us by a third party, such as a contractor, a local authority or a member of the public; or

35.4.4 an audit / review revealing that an incident had occurred.

36 ACTIONS TO TAKE ONCE AN INCIDENT HAS BEEN IDENTIFIED

36.1 Whenever an incident is identified, the following actions must be taken:

	Action	Responsibility	Timelines
1.	Report the incident to Sarah Williams the DATA Protection Officer and inform head of department	Person who was first made aware of the incident	**Immediately after the incident is identified**
2.	Investigate and identify the full details of the incident to identify the cause	Sarah Williams (with the assistance of the person who reported the incident)	**As soon as possible following the incident being reported**
3.	Identify any remedial action (see paragraph 37 below)	Sarah Williams for the Diocese, head of department and person who was made aware of incident	**As soon as possible following the incident being reported**
4.	Complete a formal Personal Data Breach Report Form and return it to Sarah Williams the DPO	Head of department or individual who was first made aware of incident or Sarah Williams DPO	**Within 48 hours of the incident being identified**

5.	Review the Personal Data Breach Report Form and determine whether the incident constitutes a Personal Data breach or a 'near miss' (i.e. an incident which does not meet the definition of a Personal Data breach)	Sarah Williams DPO	**As soon as possible following step 4**
6.	If necessary, decide whether to notify (i) the ICO; and/or (ii) individual Data Subjects, of the Personal Data breach (see paragraph 38 below)	Sarah Williams DPO	**As soon as possible following step 4**
7.	If necessary, notify the ICO of the Personal Data breach	Sarah Williams DPO	**Within 72 hours of the incident being identified**
8.	If necessary, notify individual Data Subjects of the Personal Data breach	Sarah Williams, head of department, or person who was first aware of incident, whoever is the most appropriate person	**Without undue delay (in practice this should be done as soon as possible)**

37 TAKING REMEDIAL ACTION

37.1 Following the reporting of the issue, the DPO shall advise the relevant member of personnel what remedial action must be taken, in particular where parishioners, vulnerable individuals or children are affected in any way by the Personal Data breach. Individuals may suffer distress and inconvenience where they are aware that a breach has occurred. In some cases, they may be at risk of suffering financial detriment or physical harm as a result of the breach.

37.2 Remedial action should seek to mitigate any risks the individual has been exposed to as a result of the breach, to prevent similar breaches occurring in the future and to protect the Diocese's reputation. Action will be dependent on case specifics.

If there is any doubt at all about the remedial action required to be taken, the DPO must contacted

37.3 Remedial action might include the following:

37.3.1 if Personal Data is in the hands of a third party, it should be retrieved from the third party or deleted from the third party's IT system then please notify the Finance Department in the Curial Office it might be necessary to contact the IT Consultant for assistance;

37.3.2 if the breach arose as a result of an IT issue, the source of the issue should be identified and rectified, please notify the Finance Department in the Curial Office it might be necessary to contact the IT Consultant for assistance;

37.3.3 if the breach arose as a result of human error, the individual at fault should be made aware of the error and where appropriate asked to undertake additional training or (only in the most serious cases) be subjected to disciplinary action.

38 NOTIFYING A PERSONAL DATA BREACH

38.1 Under the GDPR, there is an obligation to report a Personal Data breach to the Information Commissioner's Office (ICO) 'without undue delay' and in any event within 72 hours of the Archdiocese becoming aware of the breach.

38.2 There is an exception to this reporting requirement where the Personal Data breach is unlikely to result in a risk to the rights and freedoms of the individuals affected. A decision on whether the breach must be reported to the ICO will be made by the Data Protection Officer who will notify Trustees of the situation and who will form an independent view about the appropriate steps to be taken, following receipt of the Personal Data Breach Report Form; copies of which are available in the Data Protection file and from the finance office.

38.3 Where the Personal Data breach is likely to result in a high risk to the rights and freedoms of individuals affected, there is an obligation to notify those individuals of the breach 'without undue delay'. A Personal Data breach that may result in a high risk to individuals may include where an individual is exposed to the risk of suffering financial detriment or physical harm if they are not notified of the breach. Where this is the case, then the Data Protection Officer must inform them of the breach by letter. The Data Protection Officer will make the final decision as to whether notifying individuals is required and what explanation is provided to them.

38.4 Where individuals are aware that they are the subject of a Personal Data breach, then they must be contacted promptly. Brief details of the remedial action taken should be provided to reassure them, where this information can be provided without revealing any personal or confidential information.

38.5 Where appropriate, remedial action should also be considered for any other individuals who may also have been affected indirectly.

38.6 The Data Protection Officer will decide whether or not the affected individuals should also be sent a written apology to minimise reputational damage. This decision will be taken in conjunction with the insurers.

38.7 As well as the requirement to report Personal Data breaches to the ICO, it may also be necessary to report them to other authorities such as the Police and to the Diocese's insurers. These actions should only be undertaken following consultation with the Data Protection Officer.

39 FOLLOW-UP ACTION

39.1 To ensure that we learn from our mistakes, the parish, individual or group responsible is required not only to confirm that remedial action has taken place, but also that the causes of the Personal Data breach have been analysed and action has been taken to ensure similar breaches do not occur again. Confirmation of this action will be reported and saved by the Data Protection Officer as an audit trail.

40 CENTRAL LOGGING OF THE ISSUE

40.1 Once the parish, individual or group responsible has confirmed that remedial action and any appropriate follow-up action has been taken, provided that:

40.1.1 the individual being satisfied with the remedial action taken in respect of the breach; and

40.1.2 Data Protection Officer being satisfied that regulatory procedures have been followed;

40.1.3 then the breach can be marked as closed by the Data Protection Officer.

40.2 A copy of all breach forms will be kept by the Data Protection Officer and stored at the Curial Office.

41 GLOSSARY

"**Data Controller**" means a person, organisation or body that determines the purposes for which, and the manner in which, any Personal Data is processed. A Data Controller is responsible for complying with the data protection laws including the GDPR and establishing practices and policies in line with them.

"**Data Processor**" means any person, organisation or body that Processes personal data on behalf of and on the instruction of the Archdiocese. Data Processors have a duty to protect the information they process by following data protection laws.

"**Data Subject**" means a living individual about whom the Archdiocese processes Personal Data and who can be identified from the Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data and the information that the Archdiocese holds about them.

"**Personal Data**" means any information relating to a living individual who can be identified from that information or in conjunction with other information which is in, or is likely to come into, the Archdiocesan possession. Personal Data can be factual (such as a name, address or date of birth) or it can be an opinion (e.g. a performance appraisal). It can even include a simple email address. A mere mention of someone's name in a document does not necessarily constitute Personal Data, but personal details such as someone's contact details or salary (if it enabled an individual to be identified) would fall within the definition.

"**Processing**" means any activity that involves use of Personal Data. It includes obtaining, recording or holding the information or carrying out any operation or set of operations on it, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring or disclosing Personal Data to third parties.

"**Special Categories of Personal Data**" (previously called sensitive personal data) means information about a person’s racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexuality. It also includes genetic and biometric data. Special Categories of Personal Data can only be processed under strict conditions and such processing will usually, although not always, require the explicit consent of the Data Subject.

PERSONAL DATA BREACH FORM FOR ARCHDIOCESE OF SOUTHWARK

PART 1

TO BE COMPLETED BY THE DEPARTMENTAL OR LINE MANAGER OR DATA PROTECTION OFFICER (''THE DPO'')

1 WHO WAS FIRST MADE AWARE OF THE INCIDENT?

2 DATE REPORTED TO APPROPRIATE MANAGER AND DPO

3 DATE OF BREACH?

4 HOW THE BREACH WAS IDENTIFIED?

5 PLEASE GIVE A DESCRIPTION OF THE BREACH AND THE NATURE OF THE BREACH?

6 HOW MANY PEOPLE WERE AFFECTED?

7 PLEASE GIVE A DESCRIPTION OF THE DATA AFFECTED

8 WHAT ARE THE POTENTIAL REMEDIAL ACTIONS THAT CAN BE TAKEN TO REMEDY THE

9 DATE REPORTED TO THE DIOCESE?

PART 2

TO BE COMPLETED BY THE APPROPRIATE MANAGER OR DPO (WITH THE INDIVIDUAL'S ASSISTANCE)

10 IS THE INCIDENT A 'NEAR MISS'? IF SO WHY?

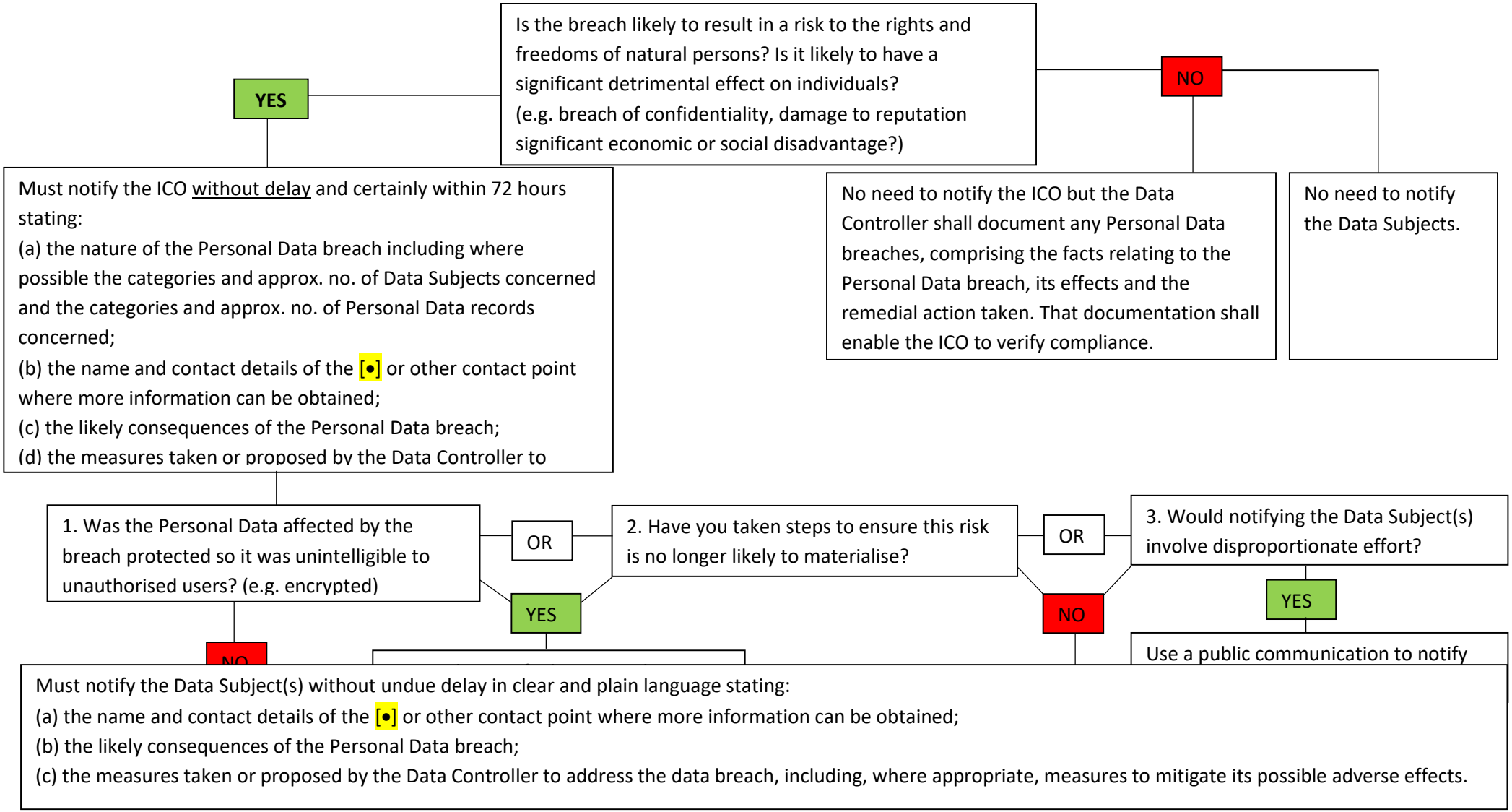
11 DOES THE INCIDENT CONSTITUTE A PERSONAL DATA BREACH?

12 WHAT REMEDIAL ACTION HAS BEEN TAKEN?

13 IS IT NECESSARY TO NOTIFY THE INFORMATION COMMISSIONER'S OFFICE? IF YES WHAT DATE WAS THIS DONE?

14 IS IT NECESSARY TO NOTIFY INDIVIDUALS DATA SUBJECTS OF THE BREACH? IF NO, WHY NOT? IF YES WHAT DATE WAS THIS DONE?

Signed: …… Date……


Is the breach likely to result in a risk to the rights and freedoms of natural persons? Is it likely to have a significant detrimental effect on individuals? (e.g. breach of confidentiality, damage to reputation significant economic or social disadvantage?)
YES
NO
Must notify the ICO without delay and certainly within 72 hours stating:
(a) the nature of the Personal Data breach including where possible the categories and approx. no. of Data Subjects concerned and the categories and approx. no. of Personal Data records concerned;
(b) the name and contact details of the [•] or other contact point where more information can be obtained;
(c) the likely consequences of the Personal Data breach;
(d) the measures taken or proposed by the Data Controller to
No need to notify the ICO but the Data Controller shall document any Personal Data breaches, comprising the facts relating to the Personal Data breach, its effects and the remedial action taken. That documentation shall enable the ICO to verify compliance.
No need to notify the Data Subjects.
1. Was the Personal Data affected by the breach protected so it was unintelligible to unauthorised users? (e.g. encrypted)
OR
2. Have you taken steps to ensure this risk is no longer likely to materialise?
OR
3. Would notifying the Data Subject(s) involve disproportionate effort?
YES
NO
YES
NO
Use a public communication to notify
Must notify the Data Subject(s) without undue delay in clear and plain language stating:
(a) the name and contact details of the [•] or other contact point where more information can be obtained;
(b) the likely consequences of the Personal Data breach;
(c) the measures taken or proposed by the Data Controller to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

PRIVACY NOTICE FOR EMPLOYEES ARCHDIOCESE OF SOUTHWARK

58 ABOUT THIS DOCUMENT

58.1 During the course of our business activities we process personal data (which may be held on paper, electronically, or otherwise) about our employees and other workers, and we recognise the need to process such data lawfully, fairly and in a transparent manner. The purpose of this policy is to make you aware of how we will do so.

58.2 This policy does not form part of any employee's or other worker's contract of employment or engagement and we may amend it at any time.

59 DETAILS ABOUT US

59.1 We are the Archdiocese of Southwark a registered charity in England and Wales with number 1173050.

59.2 The current legislation that applies to our processing of personal data is the Data Protection Act 1998 ("DPA"). As from 25th May 2018, the DPA will be replaced by the EU General Data Protection Regulation ("GDPR"), supplemented by legislation currently going through Parliament, which is likely to become the Data Protection Act 2018 ("New DPA"). This policy aims to comply with both the DPA and, when in force, the GDPR and the New DPA, and these laws are together referred to in this policy document as the "Data Protection Legislation".

59.3 The Archdiocese is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to Sarah Williams, the Data Protection Officer.

60 PERSONAL DATA WE MAY COLLECT AND PROCESS

60.1 In connection with the employment or engagement by the Archdiocese of Southwark of our employees and other workers, we will collect and process the categories of personal data relating to our employees and other workers set out in the Schedule to this policy. This may include data we receive directly from an employee or worker (for example, when they complete forms or correspond with us by mail, phone, email or otherwise) or from other sources (including, for example, third parties who provide employment references, customers, clients, suppliers and others), as well as Governmental and Regulatory or other authorities. Other personal data may be produced, such as employment and disciplinary records, to enable us to meet our legal obligations as an employer (for example to pay you), monitor your performance and to confer benefits in connection with your employment.

60.2 "Personal data" means recorded information we hold about you from which you can be identified. It may include contact details, other personal information, photographs, expressions of opinion about you, or indications as to our intentions about you. "Processing" means doing anything with the data, such as accessing, disclosing, destroying or using the data in any way.

60.3 The purposes for which we process the personal data of employees and other workers, and the legal basis on which we do so, will vary according to the category of personal data concerned. In most cases, the processing we carry out will be necessary:

60.4 for the performance of the contract of employment or engagement to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into the contract; or

60.5 for compliance with a legal obligation to which we are subject; or

60.6 for the purposes of the legitimate interests pursued by the Archdiocese or by a third party, provided such interests are not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

60.7 In certain cases, we will process the personal data where the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

60.8 In exceptional cases, processing may be necessary in order to protect the vital interests of the data subject or of another natural person.

60.9 The basis on which we will usually process personal data relating to employees and other workers (based on paragraph 3.3 (a), (b) and (c) above) is set out in the Schedule to this policy, in each case by reference to the category of personal data in question; in the case of personal data processed for the purposes of the legitimate interests pursued by the Archdiocese, it sets out what those interests are.

60.10 The Schedule also sets out the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period, and when it will be erased.

61 SENSITIVE PERSON DATA ETC

61.1 We will only process "sensitive personal data" (also called "special categories of data" under the GDPR) about ethnic origin, political opinions, religious or similar beliefs, trade union membership, health, sex life, criminal proceedings or convictions, where a further condition is also met. Usually this will mean that you have given your explicit consent, or that the processing is necessary for the purposes of performing our obligations as the data controller or to enable you to exercise your rights as the data subject under employment law, social security law or the law relating to social protection, or for health or social care purposes.

61.2 Examples of how we may process sensitive personal data relating to employees and other workers include, as appropriate:

61.3 where we process information about an employee's or worker's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's or worker's fitness for work; or

61.4 where we process information about the employee's or worker's racial or ethnic origin or religious or similar information, in order to monitor compliance with equal opportunities legislation.

61.5 Information about criminal convictions will only be relevant in the case of employees or other workers with responsibilities that mean that special checks are justified, for example, criminal record checks on those working with children. For this reason, this issue is not further dealt with here.

62 DISCLOSURE AND SHARING OF PERSONAL INFORMATION

62.1 We may disclose personal data we hold to third parties:

62.2 if we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation; or

62.3 in order to enforce or apply any contract with the data subject or other agreements; or

62.4 to protect our rights, property, or safety of our employees, customers, or others, including exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction, in which case the processing would be necessary for the purposes of the legitimate interests pursued by the Diocese, namely in order to achieve those ends.

62.5 We may also share personal data we hold with selected third parties for the purposes set out in the Schedule, for the purposes of the legitimate interests pursued by the Archdiocese, as set out in the Schedule.

63 DATA PROTECTION PRINCIPLES – OUR OBLIGATIONS

63.1 We will ensure that your personal data is:

63.2 processed fairly and lawfully and in a transparent manner;

63.3 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

63.4 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

63.5 accurate and, where necessary, kept up to date;

63.6 kept in a form which permits identification of data subjects for no longer than necessary for the purpose;

63.7 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

63.8 not transferred to people or organisations situated in countries without adequate protection, unless there are appropriate safeguards in place, and enforceable data subject rights and effective legal remedies for data subjects are available.

63.9 We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

63.10 We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

63.11 We will process all personal data in line with the data subjects' rights.

63.12 We will process all personal data relating to employee and other workers that we hold in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measure.

63.13 We will ensure that personal data relating to employee and other workers will only be transferred to a data processor that provides sufficient guarantees to implement appropriate technical and organisational measures so that processing meets the requirements of the Data Protection Legislation and ensures the protection of the rights of the data subjects, and under a written contract that sets out (amongst other things) the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal

data and categories of data subjects, and the obligations and rights of our organisation as data controller.

64 YOUR RIGHTS AS A DATA SUBJECT

64.1 As a data subject, you have certain enforceable rights under the Data Protection legislation, including:

64.2 the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed; and

64.3 if so, access to the personal data, plus a copy of the personal data undergoing processing.

64.4 You also have the right to ask for information as to:

64.5 the purposes of the processing of your personal data;

64.6 the categories of personal data concerned;

64.7 the recipients or categories of recipient of the data;

64.8 the envisaged period for which the personal data will be stored or, if that is not possible, the criteria used to determine that period;

64.9 where the personal data was not collected from yourself as the data subject, any available information as to their source; and

64.10 where personal data is transferred to a third country, the safeguards relating to the transfer.

64.11 In addition, as a data subject you have:

64.12 the right ("right of rectification") to obtain from us as the controller without undue delay the rectification of inaccurate personal data concerning yourself and (taking into account the purposes of the processing) the right to have incomplete personal data completed;

64.13 the right ("right of erasure") to obtain from us as the controller the erasure of personal data concerning yourself without undue delay, where:

64.14 the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; or

64.15 the processing is based on your consent as the data subject, and you withdraw that consent (and there is no other legal basis for processing); or

64.16 the processing is based on its being necessary for our legitimate interests as the data controller or those of a third party, and you as the data subject object to the processing, unless we demonstrate that the processing is based on compelling legitimate grounds which override your interests, rights and freedoms as the data subject, or that it is for the establishment, exercise or defence of legal claims;

64.17 the right ("right of restriction") to obtain from us as the controller the restriction of processing where the data is inaccurate, unlawfully processed, no longer required except for the establishment, exercise or defence of legal claims, or pending the verification whether we have legitimate grounds as the controller which override your rights as the data subject;

64.18 the right ("right of portability") to receive the personal data concerning yourself, which you have provided to us as the data controller, in a structured, commonly used and machine-

readable format, and to transmit the data to another controller, where the processing is based on consent or carried out by automated means;

64.19 the right ("right to object") to object to processing based on our legitimate interests as the data controller, where these are outweighed by your interests, rights and freedoms as the data subject, unless the processing is required for the establishment, exercise or defence of legal claims;

64.20 the right not to be subject to a decision based solely on automated processing, including profiling; and

64.21 the right to make a complaint to the supervisory authority (the Information Commissioner's Office).

64.22 For further information about your rights as a data subject, please contact Sarah Williams.

64.23 Changes to this policy

64.24 We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

SCHEDULE OF DATA PROCESSING ACTIVITIES

Type of data subject	**Type of data**	**Type of processing**	**Purpose of processing**	**Legal basis of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**
Employees/ Workers	Name Address Telephone number Date of Birth Personal email address, work email address, Salary Benefits Bank details National insurance number Passport, visa, nationality Medical disclosure Employment/education history Student loan information, court deductions,	Information held on personnel files and payroll spreadsheets (electronic) and in archive boxes and paper personnel files for use in payroll and employee management.	Storage of historic and current personal and employment documentation of employees, paper copies of current employment documentation	This processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of employees in the field of their employment. It is necessary for the performance of a contract to which the data subject is party.	Internal – Shared with HR External: Insurance companies relevant to employee insurance Outsourced payroll HMRC Home Office Organisations dealing With childcare vouchers, benefits	**7 years from last day of service**

	Pension Gender Vehicle registration number Childcare vouchers, GAYE, cycle scheme DIS beneficiary information Employment references Disciplinary/capability records, Employee correspondence References				in kind and student loans DBS checking organisation A full list of third parties is available on request	
Employees/ Workers	Special Categories of Personal Data: CRB check information, criminal conviction disclosure	Information held on personnel files and payroll spreadsheets (electronic) and in archive boxes and paper personnel files for use in payroll and employee management.	The processing is necessary for the purposes of performing or exercising obligations or rights of the Diocese as the employer or the data subject under employment law, social security law or the law relating to social protection and the	Storage of historic and current personal and employment documentation of employees, paper copies of current employment documentation.	Internal – Shared with HR External: Insurance companies relevant to employee insurance Outsourced payroll	**Personnel and health records 7 years after last day of service.** **HMRC information will be retained in accordance with legislation currently 6 years**

			Diocese has an appropriate policy in place.		HMRC Home Office Organisations dealing With childcare vouchers, benefits in kind and student loans DBS checking organisation A full list of third parties is available on request	**after last day of service** **DBS searches and information relating safeguarding employees, or employees involved with safeguarding will be retained in accordance with law for a minimum period of 75 years.**