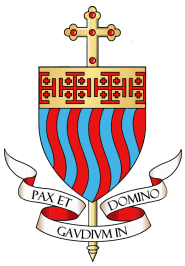


THE CATHOLIC DIOCESE OF
ARUNDEL & BRIGHTON

DATA PROTECTION HANDBOOK

Version: October 2022

CONTENTS

DATA PROTECTION POLICY

1. INTRODUCTION AND BACKGROUND

1.1 The Diocese of Arundel & Brighton (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2016/679 (the "GDPR") and any other relevant data protection legislation, domestic or otherwise, (as may be in force or repealed or replaced from time to time) (together the "Data Protection Rules").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, and to demonstrate compliance, 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 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 paragraph 10 of this Policy.

3.2 The Diocese is responsible for paying to the ICO any data protection fees levied on Data Controllers by the Data Protection Rules.

3.3 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 the Diocese's data protection policies and procedures and their own responsibilities in terms of data protection, and understand that failure to comply may result in disciplinary sanctions in the event of non-adherence or breach; and

4.1.9 adopt, monitor and keep under review, a data retention schedule which sets out the periods for which different categories of Personal Data will be kept.

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.

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) and will consider other regulation relevant to data protection, such as the Privacy and Electronic Communications Regulations. Please contact the DPO for guidance (see paragraph 10 of this Policy).

5. DATA SECURITY & RESPONSIBILITIES OF CLERGY, STAFF AND VOLUNTEERS

5.1 The Diocese shall 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 is stored only on the central Diocesan computer system and not on individual PCs, portable electronic devices or removable storage media, unless those devices are compliant with the BYOD Policy OR are subject to appropriate measures of password protection, encryption and remote deletion;

5.1.3 passwords are kept confidential 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 Further detail on the Diocese's requirements in relation to IT security are set out in the Computer Usage Policy.

5.3 In the event that you become aware that there has been a Data Breach, you must report this immediately to the Diocesan Data Protection Officer (a function covered by the Chief Operating Officer) following the Data Breach Procedure. Further contact details for the DPO can be found in paragraph 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.

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 Where an individual signs a list at the back of church to confirm being able to assist at a parish event 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 funeral data to invite families for an annual Mass of rememberance

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	Using parishioners' health-related data for pastoral visits 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

Lawful Ground for Processing of Special Categories of Data	Examples
Where the Diocese is exercising obligations or rights which are imposed or conferred by law on it or the data subject in connection with employment, social security or social protection and the Diocese has an appropriate policy document in place	To undertake appropriate checks on individuals prior to taking up a role in the Diocese, including but not limited to staff in the safeguarding department or working with individuals who are vulnerable For health & safety reasons and to ensure that Charity Commission procedures are complied with and to protect Diocesan assets, especially in relation to those employees who handle money, or to comply with professional obligations.
Where it is necessary for the prevention or detection of an unlawful act	For example, preventing fraud, passing on information to the Police or other investigatory body, such as HM Revenue & Customs, for Tax and other financial purposes such as fraud, or for Border Control purposes
Where the Diocese is complying with or assisting others to comply with regulatory requirements relating to unlawful acts or dishonesty	Passing on information to the Police or other investigatory body including the Benefits Agency, HM Revenue & Customs, external professional and regulatory organisations. For health & safety reasons and to any other external regulatory authority
Where it is carried out in the course of safeguarding children or other individuals at risk	Making a safeguarding disclosure, maintaining safety and reducing the prospect of risk
Where information is disclosed for insurance purposes	Ensuring the Diocese has appropriate insurance cover
Where an individual has given their consent to the processing	For example, if it is necessary to provide information as part of an inspection or audit, or as part of a tender, or during the course of business and/or related charitable functions
Where the Diocese is establishing, exercising or defending legal claims	Providing information to our insurers or lawyers in connection with legal proceedings, in the Courts, Tribunals or other legal proceedings
Where it is necessary to protect the vital interests of an individual	Passing on information to the Police, the NHS or a carer or next of kin if appropriate.
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 pastoral activities, or in accordance with delivering charitable purpose.

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 and undertakings as to the inception and maintenance of appropriate measures of protection as well as insurance cover. 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 European Economic Area ("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, dicastery or appellate tribunal exercising canonical jurisdiction) . Additionally, such transfers can only take place on a number of legal grounds. The Diocese does not store Personal Data outside of the UK. However, the Diocese may transfer Personal Data outside of the EEA where requested by the Data Subject, on the basis of the Data Subject's informed consent. This includes, but is not limited to, the situation where a Data Subject requires their marriage record to be sent to a non-EEA country. 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. If a verbal Subject Access Request is made, the person receiving this request must record it in writing and alert the DPO without delay.

7.5.3 All Subject Access Requests will be dealt with by the DPO. Clergy, employees or volunteers who receive a Subject Access Request 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 'Direct Marketing' includes all advertising and promotional activities, including promoting the aims and ideals of not-for-profit organisations.

8.2 Any use of Personal Data for marketing (including fundraising) purposes must comply with the Data Protection Rules and the Privacy and Electronic Communications Regulations (EC Directive) 2003 ("PECR") (and any replacement legislation), which relate to marketing by electronic means.

8.3 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.

8.4 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).

8.5 In the event of any such activity being undertaken, reference will be made to the guidance issued by the Information Commissioner's Office and the principles set out therein will be adhered to.

9. MONITORING AND REVIEW

9.1 This policy will be reviewed within two years and may be subject to change.

10. CONTACTS

10.1 Any queries or complaints regarding data protection generally or this Policy specifically should be addressed to the diocesan Data Protection Officer; this function is being supported by the diocesan Chief Operating Officer, Sarah Kilmartin, who can be contacted here E: coo@abdiocese.org.uk, by T: 01293 651145 or at the following address:

10.2 The St. Philip Howard Centre, 4 Southgate Drive, Crawley RH10 6RP.

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 the policies below and any other relevant procedural or employment policy:

11.1.1 Privacy Notice

11.1.2 Data Retention Schedule

11.1.3 Whistleblowing Policy

11.1.4 Safeguarding Policies

11.1.5 All employment related policies, e.g. disciplinary, grievance, sickness absence and recruitment

11.1.6 Complaints Policy

11.1.7 Fundraising Policy

11.1.8 Computer Usage Policy

11.1.9 Bring Your Own Device Policy

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 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 Diocese. 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 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 DIOCESE OF ARUNDEL & BRIGHTON

1. ABOUT THIS POLICY

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

1.2 This Policy covers all trustees of the Diocese, clergy, officers, consultants, contractors, volunteers, casual workers, agency workers, parishioners, and anyone who has access to our IT and communication systems. In this policy all of these people are referred to as Diocesan Personnel.

1.3 Misuse of IT and communications systems can damage the Diocese and our reputation as well as causing harm and distress to any affected individuals. Breach of this Policy by employees 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.

1.4 This Policy does not form part of any contract between you and the Diocese and we may amend it at any time.

2. PERSONNEL RESPONSIBLE FOR THE POLICY

2.1 The Diocesan trustees have overall responsibility for the effective operation of this Policy and for ensuring compliance with the relevant statutory framework.

2.2 All Diocesan Personnel have a specific responsibility to ensure the fair application of this Policy and are responsible for supporting colleagues and ensuring its success.

2.3 The Diocese 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. Requests for permission or assistance should be made to your line manager; queries or requests for assistance which can't be dealt with by your department head should be reported to the IT Department in The St. Philip Howard Centre, Crawley.

3. EQUIPMENT SECURITY AND PASSWORDS

3.1 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.

3.2 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 the Diocesan network should only be allowed to use devices under supervision.

3.3 The Diocesan IT Manager will generally be responsible for making sure the software on each Diocesan device is kept up to date and that data on those devices is regularly backed up. You are responsible for making sure that software is updated and data backed up on any of your own devices used for Diocesan purposes - for further details please refer to our BYOD Policy.

3.4 The central diocesan systems are secured using two factor authentication.

3.5 You should use passwords or other security measures on all IT equipment, particularly items that you take out of the office. Passwords should be at least 8 characters long, contain numbers, lower and upper-case letters and a symbol.

3.6 You must keep your passwords confidential and must not use another person's username and password or make available or allow anyone else to log on using your username and password. When you cease to be a member of Diocesan personnel (for any reason) you must provide details of your passwords to the Chief Operating Officer or the Diocesan IT Manager and return any equipment, key fobs or cards.

3.7 If you have been issued with a laptop, tablet computer, 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. All diocesan computers are encrypted in case of loss or theft.

4. SYSTEMS AND DATA SECURITY

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

4.2 Diocesan devices are protected by anti-virus software. You must not attempt to disable these in order to download or install software from external sources without authorisation from the Diocesan IT Manager. This includes software programmes, instant messaging programmes, screensavers, photos, video clips and music files. Incoming files and data are virus-checked by software installed by the Diocese before they are downloaded. If in doubt, staff should seek advice from the Diocesan IT Manager. You must not attach any device or equipment to our systems without authorisation. 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.

4.3 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 the Diocesan IT Manager 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.

4.4 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 role.

4.5 You must be particularly vigilant if you use our IT equipment outside Diocesan premises 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.

4.6 If you have a smartphone this needs to have tracking enabled so it can be traced if lost or stolen. In addition, smartphones should be able to be deactivated remotely if lost or stolen. For further details please refer to our BYOD Policy.

5. EMAIL

5.1 Although email is a vital communication 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.

5.2 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 member of Diocesan personnel via email should inform their line manager or the Chief Operating Officer immediately.

5.3 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. Remember that data protection legislation gives everyone about whom the Diocese holds personal data the right to be to see all that personal data. This means that any comments made about a person in an email may be seen by that person.

5.4 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.

5.5 In general, you should not:

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

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

5.5.3 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;

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

5.5.5 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;

5.5.6 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;

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

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

5.6 When sending bulk distribution emails all addressees should be blind copied so that other addressees cannot see who else has been sent the email.

5.7 If you receive an email in error you should inform the sender. If you have sent an email in error you are advised to contact the DPO to discuss whether a data breach has occurred.

5.8 Do not use your own personal email account to send or receive emails which relate to your role in the Diocese. Only use the email account we have provided for you.

6. USING THE INTERNET

6.1 Internet access is provided primarily for the purposes of the Diocese. Occasional personal use may be permitted as set out in paragraph 7.

6.2 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 the Diocese, 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.

6.3 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.

6.4 Except as authorised in the proper performance of your role, 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.

6.5 The following must not be accessed from our network unless for work purposes: online radio, audio and video streaming, instant messaging, webmail (such as Gmail or Hotmail), document storage applications such as personal Dropbox accounts and social networking sites unless required for your Diocesan role. These include, but are not limited to, Facebook, Twitter, YouTube, Google+, Instagram, SnapChat, Pinterest, Tumblr, Second Life. This list may be modified from time to time.

7. PERSONAL USE OF OUR SYSTEMS

7.1 The Diocese permits 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. The Diocese may withdraw permission for it at any time or restrict access at its discretion.

7.2 Personal use must meet the following conditions:

7.2.1 use must be minimal and if you are an employee must take place substantially out of normal working hours that is, during lunch hours, before 9am or after5 pm;

7.2.2 personal emails should be labelled "personal" in the subject header;

7.2.3 use must not interfere with the work of the Diocese or with the exercise of your role within the Diocese;

7.2.4 use must not commit the Diocese to any marginal costs; and

7.2.5 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.

7.3 You should be aware that personal use of our systems may be monitored (paragraph 8) and, where breaches of this Policy are found, action may be taken under the Disciplinary Procedure (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.

8. MONITORING

8.1 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.

8.2 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 Diocese, including for the following purposes (this list is not exhaustive):

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

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

8.2.3 to assist in the investigation of alleged wrongdoing; and

8.2.4 to comply with any legal obligation.

9. PROHIBITED USE OF DIOCESAN SYSTEMS

9.1 Misuse or excessive personal use of Diocesan telephone or email systems or inappropriate internet use is not permitted and will if you are an employee be dealt with under our Disciplinary Procedure. Misuse of the internet can in some circumstances be a criminal offence. In particular, it is not permitted, and if you are an employee 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):

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

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

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

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

9.1.5 confidential information about the Diocese, the work of the Diocese or any member of Diocesan personnel, or parishioners (except as authorised in the proper performance of your duties);

9.1.6 any other statement which is likely to create any criminal or civil liability (for you or the Diocese); and/or

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

Any such action will be treated very seriously and if you are an employee is likely to result in summary dismissal.

9.2 If you are an employee, 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 others 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

1. INTRODUCTION

1.1 The Diocese 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 Diocesan offices or on parish premises, or while travelling.

1.2 Such devices include laptops, smartphones and tablets, and the practice is commonly known as 'bring your own device' or BYOD. The Diocese 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 Diocesan systems and Diocesan data using their own devices.

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

1.4 The Diocese, 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.

2. DATA PROTECTION AND BYOD

2.1 The Diocese 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 Diocese's Data Protection Policy.

2.2 The Diocese, 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 Diocesan data. Authorisation must be obtained from your line manager before using your own device for work.

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

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

3. THE RESPONSIBILITIES OF STAFF, CLERGY AND VOLUNTEERS

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

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

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

3.1.3 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

3.1.4 ensure that the device is not used for any purpose that would conflict with any other Diocesan Policies, including Policies that relate to safeguarding, confidentiality and general use of IT equipment.

3.2 While we will endeavour to assist individuals wherever possible, the Diocese cannot take responsibility for supporting devices not provided by the Diocese.

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

3.3.1 prevent theft and loss of Diocesan data, or the device itself;

3.3.2 keep Diocesan data confidential where appropriate;

3.3.3 maintain the integrity of Diocesan data; and

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

3.4 If you are using your own device under this Policy, you must comply with the Diocese's expectations for data security. You must:

3.4.1 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 Diocesan or parish emails, you must use a second, different password to log-in to the email account this is called "double-locking";

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

3.4.3 encrypt devices and content, as necessary;

3.4.4 not hold any information relating to Diocesan 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 downloaded onto your personal device. Instead, you should use your device to make use of storage and working services on systems that the Diocese offers or recommends, allowing access to Diocesan data securely over the internet.

3.4.5 where it is necessary for Diocesan 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;

3.4.6 where appropriate, ensure that Diocesan data is moved back onto the Diocesan 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 – ask for refresher training on this if you need it);

3.4.7 if Diocesan 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: use of shared cloud-based directories should generally replace the need for portable storage devices;

3.4.8 report the loss of any device containing Diocesan data or content to the Data Protection Officer (a function covered by the Chief Operating Officer) and, where possible, the Diocesan IT Manager;

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

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

3.4.11 ensure that no Diocesan 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 the Diocesan IT Manager for more guidance.

4. MONITORING AND ACCESS

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

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

4.1.2 prevent access to a particular system; and

4.1.3 take all necessary and appropriate steps to retrieve Diocesan data.

DATA BREACH PROCEDURE

1. ABOUT THIS POLICY

1.1 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."

1.2 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.

1.3 This Policy should be read in conjunction with the Diocese's Data Protection Policy.

2. IDENTIFYING AN INCIDENT

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

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

2.1.2 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;

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

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

3. ACTIONS TO TAKE ONCE AN INCIDENT HAS BEEN IDENTIFIED

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

	Action	Responsibility	Timelines
1.	Report the incident to the Data Protection Officer (DPO – a function covered by the Chief Operating 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	DPO (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 4 below)	DPO 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 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)	DPO	Within 48 hours of the incident being identified
5.	If necessary, decide whether to notify (i) the ICO; and/or (ii) individual Data Subjects, of the Personal Data breach (see paragraph 5 below)	DPO	As soon as possible following step 4
6.	If necessary, notify the ICO of the Personal Data breach	DPO	Within 72 hours of the incident being identified
7.	If necessary, notify individual Data Subjects of the Personal Data breach	DPO, 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)

4. TAKING REMEDIAL ACTION

4.1 Following the reporting of the issue, the DPO shall advise the relevant member of Diocese 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.

4.2 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.

4.3 Remedial action might include the following:

4.3.1 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. Please notify the COO in The St. Philip Howard Centre, Crawley.

4.3.2 if the breach arose as a result of an IT issue, the source of the issue should be identified and rectified, please notify the Diocesan IT Manager for assistance.

4.3.3 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.

5. NOTIFYING A PERSONAL DATA BREACH

5.1 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 Diocese becoming aware of the breach.

5.2 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 Diocese's finance office.

5.3 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 Diocese's 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.

5.4 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.

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

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

5.7 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 Diocese's Data Protection Officer.

6. FOLLOW-UP ACTION

6.1 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 Diocese's In-House Solicitor as an audit trail.

7. CENTRAL LOGGING OF THE ISSUE

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

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

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

7.1.3 then the breach can be marked as closed by the Diocese's Data Protection Officer.

7.2 A copy of all breach forms is kept by the Diocese's Data Protection Officer.

8. 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 Diocese. 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 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.

PERSONAL DATA BREACH FORM FOR DIOCESE OF ARUNDEL & BRIGHTON ("DIOCESE")

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 BREACH?

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?

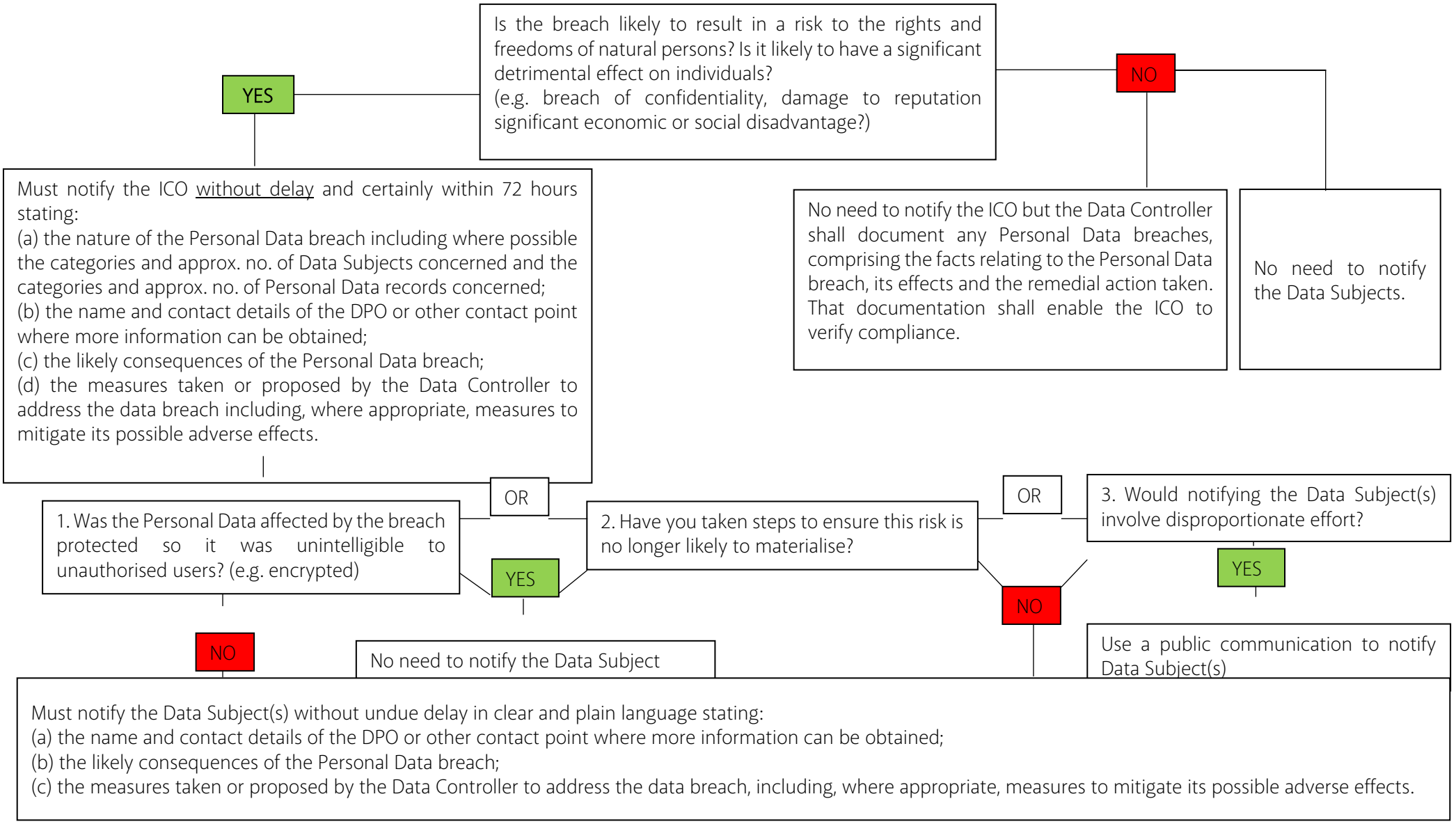
11 DOES THE INCIDENT CONSTITUTE A PERSONAL DATA BREACH?

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: ……



PRIVACY NOTICE FOR EMPLOYEES

1. ABOUT THIS DOCUMENT

1.1 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.

1.2 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.

2. DETAILS ABOUT US

2.1 We are the Diocese of Arundel & Brighton {"the Diocese"), a registered charity in England and Wales with number 252878.

2.2 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".

2.3 The Diocese 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 the Data Protection Officer (a function covered by the Chief Operating Officer), who is based at The St. Philip Howard Centre, 4 Southgate Drive, Crawley RH10 6RP.

3. PERSONAL DATA WE MAY COLLECT AND PROCESS

3.1 In connection with the employment or engagement by the Diocese of Arundel & Brighton 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 within the Diocese, 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.

3.2 "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.

3.3 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:

3.3.1 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

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

3.3.3 for the purposes of the legitimate interests pursued by the Diocese 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.

3.4 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.

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

3.6 The basis on which we will usually process personal data relating to employees and other workers (based on paragraph 3.3.1, 2 and 3 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 Diocese, it sets out what those interests are.

3.7 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.

4. SENSITIVE PERSONAL DATA ETC

4.1 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.

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

4.2.1 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

4.2.2 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.

4.3 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.

5. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

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

5.1.1 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

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

5.1.3 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.

5.2 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 Diocese, as set out in the Schedule.

6. DATA PROTECTION PRINCIPLES – OUR OBLIGATIONS

6.1 We will ensure that your personal data is:

6.1.1 processed fairly and lawfully and in a transparent manner;

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

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

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

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

6.1.6 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;

6.1.7 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.

6.2 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.

6.3 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.

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

6.5 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.

6.6 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.

7. YOUR RIGHTS AS A DATA SUBJECT

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

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

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

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

7.2.1 the purposes of the processing of your personal data;

7.2.2 the categories of personal data concerned;

7.2.3 the recipients or categories of recipient of the data;

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

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

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

7.3 In addition, as a data subject you have:

7.3.1 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;

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

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

b 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

c 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;

7.3.3 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;

7.3.4 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;

7.3.5 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;

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

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

7.4 For further information about your rights as a data subject, please contact the DPO via E: coo@abdiocese.org.uk.

8. CHANGES TO THIS POLICY

8.1 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.