

DIOCESE OF JAMAICA & THE CAYMAN ISLANDS

PERSONAL DATA BREACH POLICY

Table of Contents

PURPOSE 3
SCOPE 3
POLICY ..... **Error! Bookmark not defined.**
What is a personal data breach? ..... **Error! Bookmark not defined.**
Causes of a personal data breach 4
Discovery of a personal data breach 4
Managing and recording the breach. 5
Containment and Recovery 5
Assess and Record the Breach 5
Notifying the OIC 6
Notifying Data Subjects 6
Notifying the Police 7
Preventing future breaches 7
Monitoring and Review 7
Staff awareness and training 7
Compliance 7
APPENDIX 1 9
APPENDIX 2 10
APPENDIX 3 17

1. PURPOSE

1.1. The Diocese of Jamaica & the Cayman Islands ("the Diocese", "we" or "us") is obligated to promptly report any security breach in connection with our operations that impacts or has the potential to impact personal data as well as any violation of the data protection standards. The purpose of this policy is to set out the procedure for managing, recording, and reporting actual or suspected personal data breaches.

2. SCOPE

2.1. This policy applies to all staff and to all personal data including sensitive personal data processed by or on behalf of the Diocese. This policy is intended to supplement the Diocese's other policies such as its Data Protection Policy.

3. ROLES AND RESPONSIBILITIES

3.1. Data Protection Officer.

a) The Diocese's Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines.

b) The DPO will collaborate with the Data Breach Team to assess the severity of breaches, coordinate response efforts and notify the relevant parties.

c) The DPO will ensure that personal data breaches are identified, contained, and reported to the OIC.

3.2. Data Breach Team.

a) The Data Breach Team shall be designated to promptly respond to and manage personal data breaches.

b) This team may consist of members from various departments within the Church depending on the nature and scope of the breach.

c) The Data Breach Team will investigate the breach under the guidance of the DPO, contain its impact, and implement mitigation measures to prevent further personal data breaches.

3.3. Diocesan Council

a) The Diocesan Council is responsible for providing oversight and support for the implementation of the Personal Data Breach Policy.

b) The Council should take the necessary steps to contain breaches and mitigate the impact. The Council must assist, as best as possible, the DPO and Data Breach Team in investigating the suspected data breach.

3.4. Members of Staff of the Church

a) The Diocese expects that all members of staff, contractors, and third-party vendors operate in accordance with this policy and within the scope of their role.

b) You must report any actual, suspected, threatened or potential data breaches and incidents immediately to the DPO of the Diocese.

4. WHAT IS A PERSONAL DATA BREACH?

4.1. For the purposes of this policy, a personal data breach is defined 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.

5. CAUSES OF A PERSONAL DATA BREACH

5.1. Several factors can lead to a personal data breach:

a) Loss or theft of data or equipment on which personal data is stored, e.g., loss of a laptop or paper file;

b) inappropriate access controls allowing unauthorised use;

c) equipment failure;

d) human error, e.g., sending an email to the wrong recipient;

e) unforeseen circumstances such as a fire or flood;

f) hacking, phishing and other 'blagging' attacks where information is obtained by deceiving whoever holds it;

g) alteration of personal data without permission; or

h) loss of availability of personal data.

6. DISCOVERY OF A PERSONAL DATA BREACH

6.1. If you know or suspect a personal data breach has occurred or may occur, you should:

a) Complete the internal personal data breach report form, which is appended to this policy. The form asks for your name, but you may exclude your personal information if you wish to submit an anonymous report.

b) Email the completed form to the DPO. If you wish to make an anonymous report, you can submit the form by a non-electronic method, e.g., internal post to [ ].

6.2. You may request assistance from a Rector/Priest-in-charge to complete the personal data reach report form but must submit the report directly to the DPO.

6.3. You are not required to take any further action in relation to the breach. Particularly, you must not notify any affected individuals or regulatory authorities. The DPO will acknowledge receipt of the data breach report form (if the person making the report has given their name) and take appropriate steps to deal with the report in collaboration with the Data Breach Team (See Appendix 1).

7. MANAGING AND RECORDING THE BREACH.

7.1. On being notified of a suspected personal data breach, the Data Breach Team will conduct an initial investigation of the data incident to determine the sequence of events, ascertain facts, and assess the extent of the incident.

7.2. The Data Breach Team will take immediate steps to determine whether a personal data breach has in fact occurred. If so, the team will take appropriate action to:

a) Contain the data breach (and so far as reasonably practicable) recover or rectify the data that has been lost, damaged or disclosed;

b) Assess and record the breach in the Diocese's data breach log;

c) Notify appropriate parties of the breach; and

d) Take steps to prevent future breaches.

8. CONTAINMENT AND RECOVERY

8.1. The Data Breach Team will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data.

8.2. The Data Breach Team will identify ways to recover, correct or delete data. This may include contacting the police, e.g., where the breach involves stolen hardware or data.

9. ASSESS AND RECORD THE BREACH

9.1. Having dealt with containment and recovery, the Data Breach Team will assess the risks associated with the breach, including:

(a) what type of data is involved?

(b) how sensitive is the data?

(c) who is affected by the breach, i.e., the categories and approximate number of data subjects involved?

(d) the likely consequences of the breach on affected data subjects, e.g., what harm can come to those individuals, are there risks to physical safety or reputation, or financial loss?

(e) where data has been lost or stolen, are there any protections in place such as encryption or pseudonymisation?

(f) what has happened to the data, e.g., if data has been stolen, could it be used for harmful purposes?

(g) what could the data tell a third party about the data subject, e.g., could the loss of apparently trivial snippets of information help a determined fraudster build up a detailed picture of other people?

(h) what are the likely consequences of the personal data breach e.g., loss of reputation, loss of business, liability for fines?

(i) are there wider consequences to consider, e.g., loss of public confidence in an important service we provide?

10. Details of the breach will be recorded in the Diocese's data breach register by the Data Breach Team.

11. NOTIFYING THE APPROPRIATE PARTIES OF THE BREACH

11.1. The Data Breach Team, following consultation with the DPO, will notify:

a) The Office of the Information Commissioner (OIC);

b) Affected Data Subjects;

c) The Police where necessary; and

d) Any other parties, e.g., insurers or partners.

11.2. Notifying the OIC. The Data Breach Team will notify the OIC when a personal data breach has occurred within 72 hours after the Diocese becomes aware of it. The notification must be made in the prescribed form provided in the Appendix below or otherwise as updated under the Data Protection Act and/or regulations under that statute. If the Data Breach Team is unsure whether to report, the default position should be to report.

11.3. Notifying Data Subjects. Within 72 hours after becoming aware of the breach, the Data Breach Team will notify each data subject whose personal data is affected by the breach.

11.4. The notification must be made directly to the data subject by post, electronic mail or any other form of written communication that is reasonably appropriate in the circumstances.

11.5. If direct communication cannot be given because it would cause undue hardship to the Diocese or the Diocese does not have the contact information of the data subject, notification by indirect means may be utilized. Such indirect notification may be given by any medium of communication to which the public has access or by any means where the notification could reasonably be expected to reach the data subject concerned.

11.6. The notification must include:

a) A description of the nature of the security breach such as the date or dates which the breach occurred and details of what happened;

b) The consequences that the data subject is likely to suffer as a result of the breach including a description of the personal information that may be affected by the breach;

c) the measures taken or proposed to be taken to mitigate or address the possible adverse effects of the breach;

d) the measures recommended (if any) to be taken by the data subject to mitigate the possible negative impacts of the breach; and

e) the relevant contact information of the Data Protection Officer that the data subject can use to obtain further information about the breach.

11.7. Notifying the Police. If it is determined that the breach arose from a criminal act, under the Cybercrimes Act or otherwise, perpetrated against or by a representative of the Diocese, the Data Breach Team will notify the police and/or relevant law enforcement authorities.

12. PREVENTING FUTURE BREACHES

13. Once the personal data breach has been dealt with, in accordance with this policy, the Data Breach Team will:

a) establish what security measures were in place when the breach occurred;

b) assess whether technical or organisational measures can be implemented to prevent the breach happening again;

c) consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;

d) consider whether it is necessary to conduct a Data Protection Impact Assessment (DPIA);

e) update the Diocese's personal data risk register; and

f) debrief the Data Breach Team members following investigation.

14. MONITORING AND REVIEW

14.1. The Diocese will monitor the effectiveness of all its policies and procedures regularly, and conduct a comprehensive review and update as necessary, at least [annually].

14.2. The Diocese's monitoring and review exercises will include looking at how its policies and procedures are working in practice to reduce the risks posed to our Diocese.

15. STAFF AWARENESS AND TRAINING

15.1. Staff awareness and understanding is crucial to the success of our systems and policies. The DPO will, together with the IT department, procure regular training to staff:

a) at induction;

b) when there is any substantial change to the law, regulations or our policy;

c) when significant new threats are identified; and

d) in the event of an incident affecting the Diocese or other religious organisations.

16. COMPLIANCE

16.1. Failure to comply with this policy and associated policies puts the Diocese at risk. Failure to notify the DPO of an actual or suspected personal data breach is a very serious issue. You may be liable to disciplinary action if you fail to comply with the provisions of this, and all related plans, policies and procedures.

Approved: Diocesan Council **Date: June 18, 2026**

APPENDIX 1
DATA BREACH TEAM

Data Protection Officer	Mr. Almerick Cooke 876-926-2498 876-926-8925
Rectors/Priest-in-Charge	(As per individual congregations/Cures)
HR Officer	Mrs. Donna Evelyn 876-926-2498 876-926-8925
Director – Mission & Ministry (Matters for the Diocesan Children's Homes)	Ms. Claudette Marshall 876-926-2498 876-926-8925

APPENDIX 2

INTERNAL DATA BREACH REPORT FORM

Employees are urged to promptly report any identified data breaches. In the event of discovering a data breach, please immediately inform the DPO and the Rector/Priest-in-Charge through both email and telephone. THE DIOCESE IS OBLIGATED TO NOTIFY THE OFFICE OF THE INFORMATION COMMISSIONER OF THE PERSONAL DATA BREACH AS SOON AS THERE IS AWARENESS OF THE BREACH. Therefore, your promptness is crucial.

Please fill out this form to the best of your capability, providing as much information as you can to facilitate an initial assessment. Failure to expeditiously notify a data breach may result in disciplinary action.

Form Instructions:

1) Call the office and speak to the DPO for the Diocese at [insert DPO telephone number]
2) Complete section 1 of this form and email it to [DPO email address] The DPO will complete the remainder of the form and investigate further.

SECTION 1: NOTIFICATION OF BREACH

To be completed by the employee reporting the incident.

Name of department	
Name of employee reporting the incident	
Contact details of employee reporting the incident (email address, telephone number)	
Date and time incident was discovered	
Date(s) and time(s) on which the incident occurred	
Place of incident	

Brief description of the incident and details of any data lost	
Number of Data Subjects affected, if known.	
Has any personal data been placed at risk? If so, then please provide details.	
Brief description of any action(s) taken at the time of discovery.	
For use by the Data Protection Officer	
Received by	
Received at (date and time)	
Forwarded for action to	
Forwarded at (date and time)	

SECTION 2: ASSESSMENT OF SEVERITY

To be completed by the Data Breach Team

Details of any IT systems, equipment, devices or records involved in the breach	
What is the nature of the data lost?	
How much data has been lost?	
If a laptop is lost / stolen, then how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial, legal, liability or reputational consequences for the Organisation or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of data that fall into the following categories.	

<u>HIGH RISK</u> personal data **Sensitive personal data relating to an individual's:** **a) Genetic or biometric data** **b) Filiation, or racial or ethnic origin** **c) Political opinions, philosophical beliefs, religious beliefs** **d) Trade union membership** **e) Physical or mental health or condition** **f) Sex life** **g) Criminal history**	
Information that could be used to commit identify fraud such as; personal bank account or other financial information; national identifiers such as TRN numbers or copies of passports.	
Personal information relating to vulnerable adults and children.	

Security information that would compromise the safety of individuals if disclosed.	

SECTION 3: ACTIONS TAKEN

To be completed by the Data Protection Officer

Incident Number	
Report received by	
Report received at (date and time)	
Action taken by responsible officers(s)	
Was the incident reported to the police?	YES / NO
If YES, notified at (date and time)	

Follow up action required / recommended	
Reported to Data Protection Officer (date and time)	
Reported to other internal stakeholders (details, dates and times)	
Notification to Office of the Information Commissioner	YES / NO
If YES, notified at (date and time)	
If YES, details	
Notification to Data Subjects	YES / NO
If YES, notified at (date and time)	

If YES, details	
Notification to other external regulators / stakeholders	YES / NO
If YES, notified at (date and time)	
If YES, details	

APPENDIX 3

DATA BREACH NOTIFICATION FORM TO THE OFFICE OF THE INFORMATION COMMISSIONER

FORM 7 **(Regulation 10)**

THE DATA PROTECTION ACT, 2020

PERSONAL DATA BREACH REPORTING FORM
under section 21 of the Act

1. PARTICULARS OF DATA CONTROLLER

Name: Click or tap here to enter text.
Address: Click or tap here to enter text.
Contact Person: Click or tap here to enter text.
Phone Number: Click or tap here to enter text.
Email: Click or tap here to enter text.
Scope: ☐Private ☐ Public ☐ Other (*please specify*)
……..

2. PARTICULARS OF DATA PROTECTION OFFICER OR REPRESENTATIVE

Name: Click or tap here to enter text.
Address: Click or tap here to enter text.
Phone Number: Click or tap here to enter text.
Email: Click or tap here to enter text.
Scope: ☐ Private ☐ Public ☐Other *please specify*)
……..……..

3. PARTICULARS OF DATA PROCESSOR (if applicable)

Name: Click or tap here to enter text.
Address: Click or tap here to enter text.
Contact Person: Click or tap here to enter text.
Phone Number: Click or tap here to enter text.
Email: Click or tap here to enter text.
Scope: ☐Private ☐ Public ☐ Other (please specify)
……...

4. PARTICULARS OF OTHER INVOLVED ENTITY

Is there another entity involved in this data breach?
☐ Yes ☐ No
(If yes, complete the information below)

Name: Click or tap here to enter text.
Address: Click or tap here to enter text.
Contact Person: Click or tap here to enter text.
Phone Number: Click or tap here to enter text.
Email: Click or tap here to enter text.
Scope: ☐ Private ☐ Public ☐ Other (please specify)……..

5. TYPE OF REPORT

5.1 Purpose of the notification:
☐ Notify of a new personal data breach
☐ Provide more information regarding a previous report

5.2 Type of notification:
☐Comprehensive
☐In phases

Select 'comprehensive' when this notification contains all the information that the data controller has been able to gather regarding the data breach and the provision of further information is not foreseen. Select 'in phases' when this is an incomplete notification, with further information to follow.

5.3 If in phases, indicate which phase:

☐ Initial

☐Follow-up

☐Conclusive

Follow-up: The is a follow-up to an initial notification
Conclusive: This is the final information for the breach

5.4 In case of a follow-up or conclusive type of notification, please indicate, if available, the case file number provided by the Information Commissioner.

Click or tap here to enter text.

6. ABOUT THE DATA PROCESSING

6.1 Approximate number of individuals whose personal data are processed, referring exclusively to the processing activity affected by the personal data breach. Click or tap here to enter text.

6.2 The processing activity affected by the breach includes personal data about individuals:

☐In Jamaica

☐Regionally

☐Internationally/worldwide

7. DETAILS ABOUT THE BREACH AND ITS CONSEQUENCES

7.1 TIMELINE OF DATA BREACH

7.1. A Indicate the date and time on which you became aware of the breach. Click or tap to enter a date at Click or tap here to enter time.

7.1.B Is the date and time when the breach occurred known? (Where applicable, indicate date and time)

☐Actual ☐ Estimated ☐ Unknown

Date/Time: Click or tap to enter a dateat Click or tap here to enter time.

7.1.C How was the breach detected?

☐ By the data controller or data processor
☐Communication from affected data subject
☐Via social or other media
☐From third parties
☐Others:……

7.2 CAUSE

☐ Accidental or non-malicious act
☐Malicious act to damage the data controller, data processor or data subjects
☐Unknown intentionality

7.3 ORIGIN

☐ Internal: staff or systems managed by data controller
☐Internal: staff or systems managed by data processor
☐External: others, unrelated to data controller or data processor

7.4 HOW DID THE BREACH OCCUR? *(Select all relevant options)*

☐Verbal unauthorised disclosure of personal data

☐ Paper lost or stolen or left in insecure location

☐ Mail lost or opened

☐ Incorrect disposal of personal data on paper

☐ Personal data sent by mistake (postal or electronically)

☐ Personal data displayed to wrong recipient

☐ Personal data deleted/destroyed

☐ Abuse of access privileges by employee to extract, forward or copy personal data

☐E-waste (personal data still present on obsolete device)

☐ Unintended publication

☐ Sending email to multiple recipients without blind copy/distribution list

☐ Device lost or stolen

☐ Cyber incident: Encrypted device /Ransomware

☐ Cyber incident: Phishing/user account compromised

☐ Cyber incident: Unauthorised access to personal data in IT systems

☐ Technical issue

☐ Unauthorised data modification

Other:……

7.5 WHAT HAS BEEN AFFECTED AS A RESULT OF THE BREACH?

☐ Confidentiality: Persons or organisations that are not authorised, or do not have a legitimate purpose for accessing the data, have been able to access and/or extract it.

☐ Availability: Personal data have been destroyed, lost or encrypted so that they cannot be processed.

☐ Integrity: Personal data have been altered, although still accessible, but the replacement of data may result in damage to the persons concerned.

7.6 WHERE THE BREACH IS A CONFIDENTIALITY BREACH

Is the data securely encrypted, anonymised or protected so that it is unintelligible to anyone who may have had access, or individuals cannot be identified?

☐ Yes ☐ No ☐ Unknown

7.7 WHERE THE BREACH IS AN AVAILABILITY BREACH

Has the availability of the data been restored so that it can be processed as usual?

☐ Yes ☐ No ☐ Not yet, but soon

7.8 WHERE THE BREACH IS AN INTEGRITY BREACH. *(Select the most appropriate option)*

☐ Data altered, but with no evidence of illegal or wrong use.

☐ Data altered, wrongly or illegally used, but with the possibility of reversing/recovering the damages.

☐ Data altered, wrongly or illegally used, without possibility of reversing/recovering damages.

7.9 SUMMARY OF THE INCIDENT

Provide a brief description of what happened and the concrete measures taken and proposed to be taken to minimise damage to data subjects.

8. TYPE OF DATA AFFECTED

Select the types of personal data that have been affected. *(Select all applicable options)*

☐ Basic data subject identifiers (name, date of birth, contact details)
☐ User credentials (user password)
☐ Images (photo/video)
☐ National identification number
☐ Genetic data
☐ Biometric data
☐ Data revealing filiation, racial or ethnic origin
☐ Religious or philosophical beliefs
☐ Political opinions
☐ Trade union membership
☐ Health data (mental or physical)
☐ Sex life
☐ Criminal offences
☐ Economic or financial data
☐ Other: ……...

9. NUMBER OF DATA SUBJECTS AFFECTED

In total, how many data subjects were or could be affected by the breach? (*If you do not know the exact value, please give an approximate value.)*

Click or tap here to enter approximate number.

10. CATEGORIES OF DATA SUBJECTS

What are the categories of data subjects concerned? *(Select all applicable options)*

- ☐ Employees
- ☐ Customers/Clients or potential customers/clients
- ☐ Students
- ☐ Patients
- ☐ Subscribers
- ☐ Suppliers or Contractors
- ☐ Minors
- ☐ Others: ……..

11. IMPACT ON DATA SUBJECTS

From the table below indicate:

- the nature of the possible impact of the breach;
- whether there is evidence that any of the impact has occurred; and
- if the impact has not yet occurred, the assessment of the probability of the impact occurring.

NATURE OF THE POSSIBLE IMPACT	EVIDENCE THAT THE IMPACT HAS OCCURRED AS AT DATE OF NOTIFICATION	ASSESSMENT OF THE PROBABILITY OF THE IMPACT OCCURRING
☐ Limitation of their rights	☐ Yes ☐ No	☐Improbable ☐ Low ☐ High ☐ Very High ☐ Unknown
☐Inability to access a service	☐ Yes ☐ No	☐Improbable ☐ Low ☐ High ☐ Very High ☐ Unknown
☐ Identity thief	☐ Yes ☐ No	☐Improbable ☐ Low ☐ High ☐ Very High ☐ Unknown

[ATURE OF THE POSSIBLE IMPACT	EVIDENCE THAT THE IMPACT HAS OCCURRED AS AT DATE OF NOTIFICATION	ASSESSMENT OF THE PROBABILITY OF THE IMPACT OCCURRING
☐ Phishing/spamming victim	☐ Yes ☐ No	☐Improbable ☐ Low ☐ High ☐ Very High ☐ Unknown

☐ Fraud	☐ Yes ☐ No	☐Improbable ☐ Low ☐ High ☐ Very High ☐ Unknown
☐ Financial loss	☐ Yes ☐ No	☐Improbable ☐ Low ☐ High ☐ Very High ☐ Unknown
☐ Damage to reputation or relationship	☐ Yes ☐ No	☐Improbable ☐ Low ☐ High ☐ Very High ☐ Unknown
☐ Threat to professional secrecy	☐ Yes ☐ No	☐Improbable ☐ Low ☐ High ☐ Very High ☐ Unknown
☐ Humiliation or loss of dignity	☐ Yes ☐ No	☐Improbable ☐ Low ☐ High ☐ Very High ☐ Unknown
☐ Loss of control over their personal data	☐ Yes ☐ No	☐Improbable ☐ Low ☐ High ☐ Very High ☐ Unknown

☐ Discrimination	☐ Yes ☐ No	☐Improbable ☐ Low ☐ High ☐ Very High ☐ Unknown
☐Damage/Distress	☐ Yes ☐ No	☐Improbable ☐ Low ☐ High ☐ Very High ☐ Unknown
NATURE OF THE POSSIBLE IMPACT	EVIDENCE THAT THE IMPACT HAS OCCURRED AS AT DATE OF NOTIFICATION	ASSESSMENT OF THE PROBABILITY OF THE IMPACT OCCURRING
☐ Injury, Illness or loss of life	☐ Yes ☐ No	☐Improbable ☐ Low ☐ High ☐ Very High ☐ Unknown
☐ Still unknown	☐ Yes ☐ No	☐Improbable ☐ Low ☐ High ☐ Very High ☐ Unknown
☐ Other:……	☐ Yes ☐ No	☐Improbable ☐ Low ☐ High ☐ Very High ☐ Unknown

12. ACTIONS TAKEN BY THE DATA CONTROLLER AFTER THE BREACH

12.1 Have new security measures been taken after the incident that could have prevented the breach?

☐ Yes ☐ No ☐ Unknown ☐ Not Applicable

12.2 Have security policies and procedures been adapted or improved?

☐ Yes ☐ No ☐ Unknown ☐ Not Applicable

12.3 Where applicable, select only new or updated security measures:

☐ Data protection ☐ Periodic audits and information ☐ Physical access control security policies ☐ Logical access control

☐ Data protection ☐ Levels of access to data and security ☐ Data encryption training at the ☐ Backup/Recovery Plan appropriate level ☐ Anonymisation

☐ Updated IT ☐ None of the above systems

☐ Incident log

12.4 Has the incident been reported to law enforcement authorities as a criminal offence?

☐ Yes ☐ No ☐ Unknown

12.5 Have [all possible] actions been taken to resolve the breach?

☐ Yes ☐ No ☐ Unknown

12.6 Has the breach been resolved?

☐ Yes ☐ No

12.7 If yes, indicate the date on which the breach was resolved.

Click or tap to enter a date.

13. COMMUNICATION TO DATA SUBJECTS

13.1 Has the breach been communicated to the data subjects in the terms described in section 20(5) of the Data Protection Act and Regulation 10 of the Data Protection Regulations?

☐ Yes ☐ No

13.2 What means of communication was utilised? *(Select all applicable options)*

☐ Communication addressed personally to data subject (post, email, SMS, etc.)

☐ Publication on the data controller's website or social media pages

☐ Dissemination in other media

☐ Other ……..…….

13.3 Where applicable, indicate the date when information was communicated to data subjects. Click or tap to enter a date.

13.4 Where applicable, indicate the number of data subjects to whom the information was communicated. Click or tap here to enter number.

14. DELAY IN REPORTING

If there has been a delay (more than 72 hours after becoming aware of the incident and reporting it to the Information Commissioner), please provide your justifications for the delay.

Click or tap here to enter text.

Signature:
Name:
Title:
Date: