Data Breach Policy

St Paul's Church is committed to complying with data protection legislation and will take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of or damage to personal data:

If, despite the technical and organisational measures that we have put in place to protect personal data, a data security breach occurs, it is important to manage and respond to it effectively. A data security breach covers more than the simple misappropriation of data and may occur through incidents, such as:

• Loss or theft of data or equipment.

• People gaining inappropriate access.

• A deliberate attack on systems.

• Equipment failure.

• Human error.

• Catastrophic events, (for example, fire or flood).

• Malicious acts such as hacking, viruses or deception.

If such an incident occurs it is imperative that we act immediately. The following steps will be taken:

A. [Minister/Wardens] (the "Security Breach Team") will be informed immediately;

B. An investigation will be undertaken to determine:

i. The nature and cause of the breach; and
ii. The extent and nature of harm that has or could arise from the breach.

If there is no risk of harm, then no further action is required (for example if papers are temporarily lost due to being incorrectly filed but are then promptly found and no disclosure has occurred or harm likely to occur then no further action is required). If there is considered to be a risk of harm, then the following steps must be undertaken:

1. Information Commissioner's Office (ICO), must be informed within 72 hours. If we do not have all of the information by then, a report should be made within the 72 hours on the basis of what is known while investigations continue.

2. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay. Examples of this could include where there is a high risk of reputational damage, embarrassment or putting the individual's property at risk.

3. If necessary, a number of third parties will be informed which may include:

a. PCC
b. the church's insurers;
c. the police;
d. the church's solicitors.

4. Following notification we will continue to liaise and cooperate with ICO.

5. All reasonable steps to mitigate the damage arising from the breach will be taken. A record of all data protection breaches will be maintained regardless of whether or not notification is required. Detailed records of the investigation will be maintained as well. Following a breach, if necessary, it must be considered whether any of the below is required:

• Disciplinary action;
• Legal action;
• Internal review of security procedures.

A number of precedent documents have been prepared which may be of use. Please note that, where possible, legal advice should always be sought in the case of a data breach prior to sending these correspondences.

Appendix A contains a precedent letter which can be sent to a data subject on discovery of a data breach which is likely to result in a high risk of harm to the data subject and or the church/congregation (could be significant reputational damage or embarrassment or putting person(s) or property at risk).

Appendix B contains a precedent letter informing the ICO upon a data breach for which there is a risk of harm.

Appendix A INFORMING INDIVIDUAL OF A DATA BREACH

[On headed notepaper of St Paul's church]

[ADDRESSEE]

[ADDRESS LINE 1]

[ADDRESS LINE 2]

[POSTCODE]

[DATE]

Reference: PERSONAL DATA BREACH NOTIFICATION

We are sorry to inform you of a breach of security that has resulted in the [loss OR unauthorised disclosure OR destruction OR corruption – DELETE AS APPROPRIATE] of your personal data. The breach was discovered on [DATE] and is likely to have taken place on [DATE].

As a result of our investigation of the breach, we have concluded that:

The breach affects the following types of information:

[TYPES OF INFORMATION. FOR EXAMPLE, FINANCIAL, SENSITIVE PERSONAL DATA].

The information has been [accidentally or unlawfully destroyed OR lost OR altered OR disclosed without authorisation OR accessed by [[Name or Description of Organisation] OR an unauthorised person]]. [DELETE AS APPROPRIATE]

The breach occurred under the following circumstances and for the following reasons:

[CIRCUMSTANCES].

[REASONS].

We have taken the following steps to mitigate any adverse effects of the breach:

[MEASURES].

We recommend that you take the following measures to mitigate possible adverse effects of the breach:

[MEASURES].

We informed the Information Commissioner's Office of the breach on [DATE].

You can obtain more information about the breach from any of the following contact points:

St Paul's Church

[POSTAL ADDRESS].

[E-MAIL ADDRESS].

[TELEPHONE NUMBER].

[WEBSITE ADDRESS].

We apologise for any inconvenience this breach may cause you.

Yours sincerely,

.....

[NAME OF SENDER – printed under signature]

For and on behalf of St Paul's Church

Appendix B INFORMING ICO OF DATA BREACH

[On headed notepaper of St Paul's church]
[ADDRESSEE]
[ADDRESS LINE 1]
[ADDRESS LINE 2]
[POSTCODE]
[DATE]
Reference: PERSONAL DATA BREACH NOTIFICATION

I am writing to notify you of a [breach of security that resulted in the [loss OR unauthorised disclosure OR corruption OR destruction– DELETE AS APPROPRIATE] of personal data. We consider this to be a serious data security breach.
[We have investigated the breach by [DETAILS OF HOW THE BREACH WAS INVESTIGATED] and provide you with the following information.] We are in the process of investigating the breach and we anticipate completing our
investigation by [DATE], when we will provide you with the further information required. We can provide you with the following details at this stage [PROVIDE ALL THAT IS KNOWN].]
St Paul's Church is the data controller in respect of the data breach. The breach was discovered on [DATE] and is likely to have taken place on [DATE].
The information has been [accidentally or unlawfully destroyed OR lost OR altered OR disclosed without authorisation OR accessed by [[Name or Description of Organisation] OR an unauthorised person]].
[DELETE AS APPROPRIATE]
The breach occurred under the following circumstances and for the following reasons:
[CIRCUMSTANCES].
[REASONS].

Measures in place
We had the following measures in place to prevent an incident of this nature occurring:
[MEASURES].
We enclose extracts of policies and procedures that we consider to be relevant to the breach:
[EXTRACTS OF POLICES AND PROCEDURES AND DATE IMPLEMENTED].
The following were in existence at the time of the breach:
[LIST OF POLICIES AND PROCEDURES AND DATE IMPLEMENTED].

Personal data placed at risk
The breach affects the following types of information:
[TYPES OF INFORMATION, FOR EXAMPLE, FINANCIAL OR SENSITIVE PERSONAL DATA AND DETAILS OF THE EXTENT].
It is likely that the breach affects around [NUMBER] data subjects. [We have [not] informed the individuals affected by the breach because [REASONS FOR DECISION] OR The individuals are [aware OR unaware] that the incident has occurred].
The breach may have the following consequences and adverse effects on the affected data subjects:
[CONSEQUENCES].
[ADVERSE EFFECTS].
We have [received [NUMBER] of complaints OR not received any complaints] from the affected individuals.

Containment and recovery
We [have taken OR propose to take] the following measures to address the breach and to minimise and mitigate its effects on the affected individuals:
[MEASURES].
The information has [not] been recovered [and the details are as follows:
[DETAILS OF HOW AND WHEN IT WAS RECOVERED]
We have also taken the following steps to prevent future occurrences of the breach:
[REMEDIAL ACTION TAKEN].
[The facts surrounding the breach, the effects of that breach and the remedial action taken have been recorded in a data breach inventory maintained by the [PCC]

Training and guidance
We provide staff/volunteers/leaders with training on the requirements of data protection legislation [and the details are as follows:

[DETAILS OR EXTRACTS FROM TRAINING RELEVANT TO THIS DATA BREACH]
We provide detailed guidance to staff/volunteers/leaders on the handling of personal data in relation to this incident [and the details are as follows:
[DETAILS OR EXTRACTS OF ANY DETAILED GUIDANCE GIVEN TO STAFF/VOLUNTEERS/LEADERS ON THE HANDLING OF PERSONAL DATA IN RELATION TO THE DATA BREACH]
We confirm that training on the requirements under the data protection legislation is mandatory for all staff/volunteers/leaders [and that the staff members involved in this incident received training on [DATE]].

Previous contact with the Information Commissioner's Office
We have [not] reported [any] previous incidents to you within the last two years [and the details and reference numbers are as follows:
[DETAILS OF INCIDENT(S)].
[DATE(S) ON WHICH THE INCIDENT(S) WAS [WERE] REPORTED].
[THE INFORMATION COMMISSIONER'S REFERENCE NUMBER(S), IF KNOWN].

Miscellaneous
We have [not] notified any other (overseas) data protection authorities about this data breach [and the details are as follows:
[DETAILS OF DATA PROTECTION AUTHORITIES].
We have [not] informed the police about this data breach [and the details are as follows:
[DETAILS AND NAME OF POLICE FORCE].
We have [not] informed any other regulatory bodies about this data breach [and the details are as follows:
[NAME AND DETAILS OF REGULATORY BODIES].
There has [not] been [any] media coverage [and the details are as follows:
[DETAILS OF MEDIA COVERAGE].
In addition, we consider that the following information would be of interest to you:

[DETAILS].

Contact details:

If you require any further information about the breach, please contact:

[CONTACT NAME]
St Paul’s Church
[POSTAL ADDRESS]
[TELEPHONE NUMBER]
[E-MAIL ADDRESS]
[WEBSITE ADDRESS].
Yours faithfully,
.....
[NAME OF SENDER]
For and on behalf of St Paul’s Church