Data Breach Guidelines

Everyone makes mistakes but there are some things that MUST happen if you do.

This is called an **involuntary breach** and might be caused by:

- Emails are sent with recipients addresses on view; or
- Contact details are shared with a church member who is not a member of the WEBS Benefice or an officer in the Diocese of Peterborough.

Other things might also be involuntary breaches, for instance if a laptop containing member information is stolen.

If anything like this happens, or you think it may have, contact the Data Controller immediately who will advise you of what is necessary and help you. Information accidently shared within the Benefice is serious but anything externally shared might be more serious and must be properly reported.

Voluntary Breaches are likely to be rare but occur when a person in possession of the data knowingly or maliciously shares the data. This is very serious and may be an offence in law. If this has happened or you suspect it might, please contact the Data Controller immediately as this must be reported through the appropriate channels.

WEBS Benefice is required to provide the following to the supervisory authority (the diocese of Peterborough) in case of a data breach:

- A description of the nature of the personal data breach;
- The categories of personal data that have been affected by the breach;
- The number, which may be approximated if necessary, of data subjects affected by the breach;
- The number, which may be approximated if necessary, of personal data records affected by the breach;
- The name and contact details of the Data Owner (individual nominated within the Diocese as responsible for the security of that data);
- The likely outcomes of the personal data breach;
- Any measures taken by the Benefice to address and/or mitigate the breach; and
- All other information regarding the data breach.

Reporting will be done by the Data Controller with oversight from the diocese.

Keeping Data Subjects Informed

WEBS Benefice shall ensure that the following information is provided - by reference to this Data Protection Policy - to every data subject when personal data is collected:

a) Details of the charity including, but not limited to, the identity of its Data Owner;

b) The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;

c) Where applicable, the legitimate interests upon which the Benefice is justifying its collection and processing of the personal data;

d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) Where the personal data is to be transferred to one or more third parties, details of those parties;

f) Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place;

g) Details of the length of time the personal data will be held by the Benefice (or, where there is no predetermined period, details of how that length of time will be determined);

g) Details of the data subject's rights under the Regulation;

h) Details of the data subject's right to withdraw their consent to the Benefice's processing of their personal data at any time;

i) Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);

j) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;

k) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

The information set out above shall be provided to the data subject at the following applicable time:

Where the personal data is obtained from the data subject directly, at the time of collection;

Where the personal data is not obtained from the data subject directly (i.e. from another party):

a. If the personal data is used to communicate with the data subject, at the time of the first communication; or

b. If the personal data is to be disclosed to another party, before the personal data is disclosed; or

c. In any event, not more than one month after the time at which the Benefice obtains the personal data.

Data Protection Measures

The Benefice shall ensure that all its members, employees, volunteers, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

a. All emails containing personal data should be password protected and encrypted as attachments;

b. Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and the more sensitive of personal data be securely shredded with certificate provided by shredding agent.

c. Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances – if in doubt over the security of a network please seek the advice of the diocese.

d. Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

e. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;

f. Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

g. Where Personal data is to be transferred in hard copy form it should be passed directly to the recipient or sent using Royal Mail or an equivalent postal service, preferably tracked;

h. No personal data may be shared informally and if a member, employee, volunteer, agent, sub-contractor, or other party working on behalf of the Benefice requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Controller.

i. All hard copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

j. No personal data may be transferred to any members, employees, volunteers, agents, contractors, or other parties, whether such parties are working on behalf of the Benefice or not, without the authorisation of the Dara Controller;

k. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised members, employees, volunteers, agents, sub-contractors or other parties at any time;

l. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

m. No unsolicited personal data should be deliberately preserved and stored on any mobile device (including, but not limited to memory sticks, laptops, tablets and smartphones), whether such device belongs to the Benefice or otherwise without formal written approval and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.

n. No personal data should be transferred to any device personally belonging to a member, employee or volunteer and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Benefice where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the diocese that all suitable technical and organisational measures have been taken);

o. All personal data stored electronically should be encrypted and backed up with back-ups preferentially, stored offsite.

p. All electronic copies of personal data should be stored securely using passwords and data encryption;

q. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords should contain a combination of upper case and lower case letters, numbers, and symbols;

r .Under no circumstances should any passwords be written down or shared between any members, employees, volunteers, agents, contractors, or other parties working on behalf of the Benefice, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.

s. Where personal data held by the Benefice is used for marketing purposes, it shall be the responsibility of the Data Controller, to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service.

Organisational Measures

The WEBS Benefice shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

a) All members, employees, volunteers, agents, contractors, or other parties working on behalf of the Benefice shall be made fully aware of both their individual responsibilities and the Benefice's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy;

b) Only members, employees, volunteers, agents, sub-contractors, or other parties working on behalf of the Benefice that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Benefice;

c) All members, employees, volunteers, agents, contractors, or other parties working on behalf of the Benefice handling personal data will be appropriately trained to do so;

d) All members, employees, volunteers, agents, contractors, or other parties working on behalf of the Benefice handling personal data will be appropriately supervised;

e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

f) All members, employees, volunteers, agents, contractors, or other parties working on behalf of the Benefice handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;

g) All members, volunteers, agents, contractors, or other parties working on behalf of the Benefice handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant members, employees and volunteers of the Benefice arising out of this Policy and the Regulation;

h.) Where any members, volunteers, agent, contractor or other party working on of the behalf of the Benefice handling personal data deliberately and persistently fail in their obligations under this Policy, then that party shall be liable for any costs, liability, damages, loss, claims or proceedings which may arise out of that failure and hold the WEBS Benefice harmless.

Implementation of Policy

This Policy shall be deemed effective as of ……
No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Signed……..

Dated……

Review Date…….