DATA PROTECTION ACT 2018

*The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government.

*The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

Your rights

Under the Data Protection Act 2018, you have the right to find out what information the government and other organisations store about you. These include the right to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased

- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances

You also have rights when an organisation is using your personal data for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict your behaviour or interests

The Connexion has adopted the following information policy, to guard against unauthorised and unlawful processing of personal data and against accidental loss. destruction and damage.

1. No unnecessary records shall be kept in the organisation.
2. All records must be secure. This means filing cabinets or the rooms or buildings holding written and computer records should be locked. If additional security devices, such as passwords are used, so much the better.
3. Records should not be held about people who have left membership of churches for longer than necessary.
4. Records should not be given to any outside organisation (Christian or otherwise) for any purpose without the person(s) giving their permission. *(Confidential references for the purpose of education, training or employment, and appointment to office are excluded from this provision.)*
5. Right of access to one's own personal data is subject to certain conditions, such as by written application, and by payment of a £10 fee.
6. Back-up records should be kept, to make sure data is not lost by flood, fire or other catastrophe.
7. Individual church ministers and officers are responsible for the security of data held by their own churches.
8. The trustees and officers of the Connexion and Sierra Leone Mission are responsible for central information.
9. Records should be disposed of securely, such as by shredding or burning.
10. Any breaches of this policy will be investigated by the trustees.

*Full details of The Data Protection Act 2018 is available at www.gov.uk